Defence Research and Development Canada
Recherche et développement pour la défense Canada

Risk Assessment References

Documented Literature Search

Kyungryun (Cathy) Pak

Lynne Genik

DRDC Centre for Security Science

Disclaimer: The inclusion of a particular tool or methodology in this literature search should not be considered as an endorsement by DRDC. It is highly recommended that the references are reviewed before being applied or used in particular contexts or situations.

Defence R&D Canada – Centre for Security Science

Technical Note
DRDC CSS TN 2012-014

Canada

Principal Author

Kyungryun (Cathy) Pak

DRDC Centre for Security Science

Approved by

Dr. Denis Bergeron

DRDC Centre for Security Science
Section Head Decision Support

Approved for release by

Dr. Mark Williamson

DRDC Centre for Security Science
Document Review Panel Chairman

Abstract

This document presents the results of a literature search for risk assessment (RA) as it pertains to public safety and security, and was undertaken as part of a collaborative project between Defence Research & Development Canada (DRDC) and Emergency Management British Columbia (EMBC). It consists of bibliographic information, abstracts, and key points for almost 200 references, organized into the following categories: standards; frameworks and guidelines; methodologies, tools, and models; academic discussions; and case studies. The references include standards, government publications, academic papers, and reports produced by practitioners and non-governmental or private sector organizations, and were categorized, ordered and described to assist readers in selecting and retrieving references that may be of value to their work. This document is intended to be a resource for DRDC, EMBC and other external partners.

Résumé

Ce document présente les résultats d'une recherche documentaire sur l'évaluation des risques associés à la sécurité publique. Cette recherche a été menée dans le cadre d'un projet de collaboration entre Recherche et développement pour la défense Canada (RDDC) et Emergency Management British Columbia (EMBC). Des renseignements bibliographiques, des extraits et des faits saillants de près de 200 documents de références sont classés par catégorie: normes; cadre et lignes directrices; méthodologies, outils et modèles; discussions universitaires; études de cas. Les documents de références incluent des normes, des publications gouvernementales, des recherches universitaires et des rapports rédigés par des organisations professionnelles, non gouvernementales et du secteur privé. Ils ont été classés, organisés et décrits dans le but d'aider le lecteur à sélectionner et à trouver des documents de référence pouvant lui être utile. Il s'agit d'un outil que RDDC, EMBC et d'autres partenaires externes peuvent utiliser comme ressource.

Executive summary

Risk Assessment References: Documented Literature Search

Kyungryun (Cathy) Pak, Lynne Genik, DRDC Centre for Security Science; DRDC CSS TN 2012-014; Defence R&D Canada – CSS; October 2012.

Background: The collaborative project between Emergency Management British Columbia (EMBC) and Defence Research & Development Canada (DRDC) aims to demonstrate the value of a scientific approach to improving emergency management capabilities, focusing on risk assessment (RA) and critical infrastructure (CI). During the first phase of the project, DRDC performed a preliminary literature review for RA and CI and identified the need for a more extensive literature review. As a result, thorough literature searches were conducted. This paper presents the literature search for the first of these two areas, RA.

Method: The literature search was carried out primarily through Internet searches. Online databases such as the DRDC research database and the University of Ottawa library database were heavily used. In addition, several references were provided by DRDC staff and by partners. The research was conducted by searching for references on RA for all hazards and threats. The principal author read through the references and recorded bibliographic information, abstracts, and content descriptions. In addition, key characteristics of the references were noted in order to categorize and order them in a logical way.

Results: This document presents the results of a literature search in the area of RA as it pertains to public safety and security. The literature search comprises a compilation of almost 200 references, including national and international standards, government publications from various countries, academic papers, and the work of practitioners and non-governmental or private organizations. For each reference, bibliographic information, abstracts (when available), and key descriptive information are provided. In addition, the references were organized into the following categories: standards; frameworks and guidelines; methodologies, tools and models; academic discussions; and case studies.

Significance: This document addresses the need for a comprehensive literature search in the area of RA. The categorization and organization of the references in a logical order can quickly guide readers to the appropriate references. Furthermore, abstracts and descriptions will assist readers in determining the relevance of the references to their work and/or interests. Lastly, the bibliographic information is intended to allow readers to retrieve references easily. Thus, this work can be used as a resource by DRDC and external partners.

Future plans: Electronic copies of the reference documents are stored on a CSS share drive. A next step could be to create a database which would facilitate a more efficient review of the references. In addition, the collection of reference documents could be continually expanded and updated as new material is made available.

Sommaire

Documents de références sur l'évaluation des risques : Recherche documentaire

Kyungryun (Cathy) Pak, Lynne Genik, Centre des sciences pour la sécurité de RDDC; DRDC CSS TN 2012-014; R & D pour la défense Canada – CSS; Octobre 2012.

Contexte: Le projet de collaboration entre Recherche et développement pour la défense Canada (RDDC) et Emergency Management British Columbia (EMBC) vise à démontrer la valeur de l'approche scientifique pour améliorer les capacités de gestion des situations d'urgence en se concentrant sur l'évaluation des risques et les infrastructures essentielles. Au cours de la première phase du projet, RDDC a effectué une analyse documentaire préliminaire dans les deux domaines et une recherche plus approfondie s'est avérée nécessaire. Ce document présente la recherche documentaire sur l'évaluation des risques.

Méthodologie: Les recherches ont été effectuées principalement sur Internet. Des bases de données telles que celle de RDDC et celle de la bibliothèque de l'Université d'Ottawa ont été largement utilisées. De plus, des partenaires et des employés de RDDC ont fourni de nombreux documents de référence. La recherche a été menée en cherchant des références portant sur l'évaluation des risques associés à tous les dangers et les menaces. L'auteur principal a lu les ouvrages et a sauvegardé des renseignements bibliographiques, des extraits et des descriptions de contenu. Les caractéristiques principales des documents ont également été notées afin de les catégoriser et de les classer de façon logique.

Résultats: Ce document présente les résultats d'une recherche documentaire sur l'évaluation des risques associés à la sécurité publique. Plus de 200 ouvrages de référence ont été recueillis, y compris des normes nationales et internationales, des publications gouvernementales de divers pays, des recherches universitaires et des rapports rédigés par des organisations professionnelles, non gouvernementales et du secteur privé. Des informations bibliographiques, des extraits (si disponible) et des renseignements descriptifs sont fournis pour chaque ouvrage. En outre, les documents ont été classés selon les catégories suivantes : normes; cadre et lignes directrices; méthodologies, outils et modèles; discussions universitaires; études de cas.

Importance: Ce document répond au besoin en recherche documentaire exhaustive dans le domaine de l'évaluation des risques. La catégorisation et l'organisation de façon logique des références permettent aux lecteurs de trouver rapidement les ouvrages appropriés. Aussi, grâce aux extraits et aux descriptions, ils peuvent déterminer la pertinence des ouvrages à leur travail et leurs intérêts. Enfin, les renseignements bibliographiques facilitent la récupération des documents. Ainsi, les partenaires externes et le personnel de RDDC peuvent utiliser ce document comme ressource.

Futurs plans: Les versions électroniques des documents de référence sont sauvegardées sur le lecteur partagé du CSS. La prochaine étape pourrait être de créer une base de données favorisant un examen des références plus efficace. De plus, la liste des ouvrages de référence pourrait continuellement être alimentée et être mise à jour à mesure que du nouveau matériel est disponible.

Table of Contents

Acknowledgements

The authors would like to acknowledge fellow CSS staff for their support, as well as Dr. Patrick Dooley for sharing his expertise and risk assessment literature collection.

1 Introduction

1.1 Background

Defence Research and Development Canada (DRDC) provided scientific support to Emergency Management British Columbia (EMBC) for the Vancouver 2010 Olympic and Paralympic Winter Games (V2010). Following V2010, EMBC and DRDC established a collaborative project to demonstrate the value of a scientific (operational research and analysis) approach for improving emergency management capabilities. The collaborative project focuses primarily on two areas of work: risk assessment (RA) and critical infrastructure (CI).

As a first step in the project, DRDC worked on the problem definition and solution strategy, and a literature review was completed for RA and CI. This work was documented in a DRDC Technical Memorandum.[1] A more comprehensive literature search was desired and the principal author, a co-op student, was engaged to conduct and document extensive literature searches on RA and CI.

1.2 Purpose

The purpose of this paper is to present a documented literature search for RA in the context of public safety and security. The literature search for critical infrastructure is presented in a separate document.

This document is not intended to be an analytical review of the references presented in the literature search. Rather, it presents descriptive information and a categorization scheme in order to aid users in identifying references that are most valuable to their work and interests.

1.3 Scope

The literature search focuses on RA as it pertains to public safety and security. It includes standards, government publications, as well as research papers and reports produced by academia, practitioners, and non-governmental or private sector organizations. The references are mostly publications from developed countries such as Canada, the United States, the United Kingdom, Australia, New Zealand and the Netherlands, because of their similarities, applicability to the Canadian risk field and the accessibility of documents. All references presented in this literature search are unclassified, although some are only available for limited distribution.

The literature search includes references of varying scope. While some references consider all-hazards, others deal specifically with one or several hazards/threats.

Although RA was the primary focus of this literature search, it cannot be isolated from the overall framework of risk management. Hence, some of the references presented in this literature search consider risk management as a whole, of which RA is one of several elements.

This document is not a comprehensive literature search of all existing references on RA. It presents a selection of approximately 200 references which were considered to be highly relevant to public safety and security in Canada in 2012. Additional research may be required for particular topics.

[1] See Reference 5.8.4

1.4 Methodology

Research was conducted by searching for references on RA for all hazards and threats. References were retrieved through the DRDC research database and the University of Ottawa library database, and some were provided by DRDC staff and by partners.

In order to document the literature search, the principal author read the references and recorded bibliographic information as well as abstracts and key terms. When abstracts were not available or did not adequately describe the content, additional information was recorded, such as document descriptions, purpose, goals, scope, audience, and subject areas/sections. Key information and concepts were also documented, such as major steps or phases in the process of RA or risk management, hazards/threats considered, supplementary tools or resources, and recommendations.

The references were then grouped and categorized into the following themes: standards; frameworks and guidelines; methodologies, tools and models; academic discussions; and case studies. The sections were then divided into sub-categories as follows:

- Standards by international and national reach;
- Frameworks and guidelines by international, national, regional, local, and hazard-specific use, including a section for lexicons;
- Methodologies, tools and models by the scope of hazards/threats considered;
- Academic discussions by subject area;
- Case studies by the country in which the risk assessments were conducted.

This categorization scheme is illustrated in Figure 1.

Within each sub-section, the references were grouped by subject area, and then ordered by country of origin and chronology (most recent to least recent).

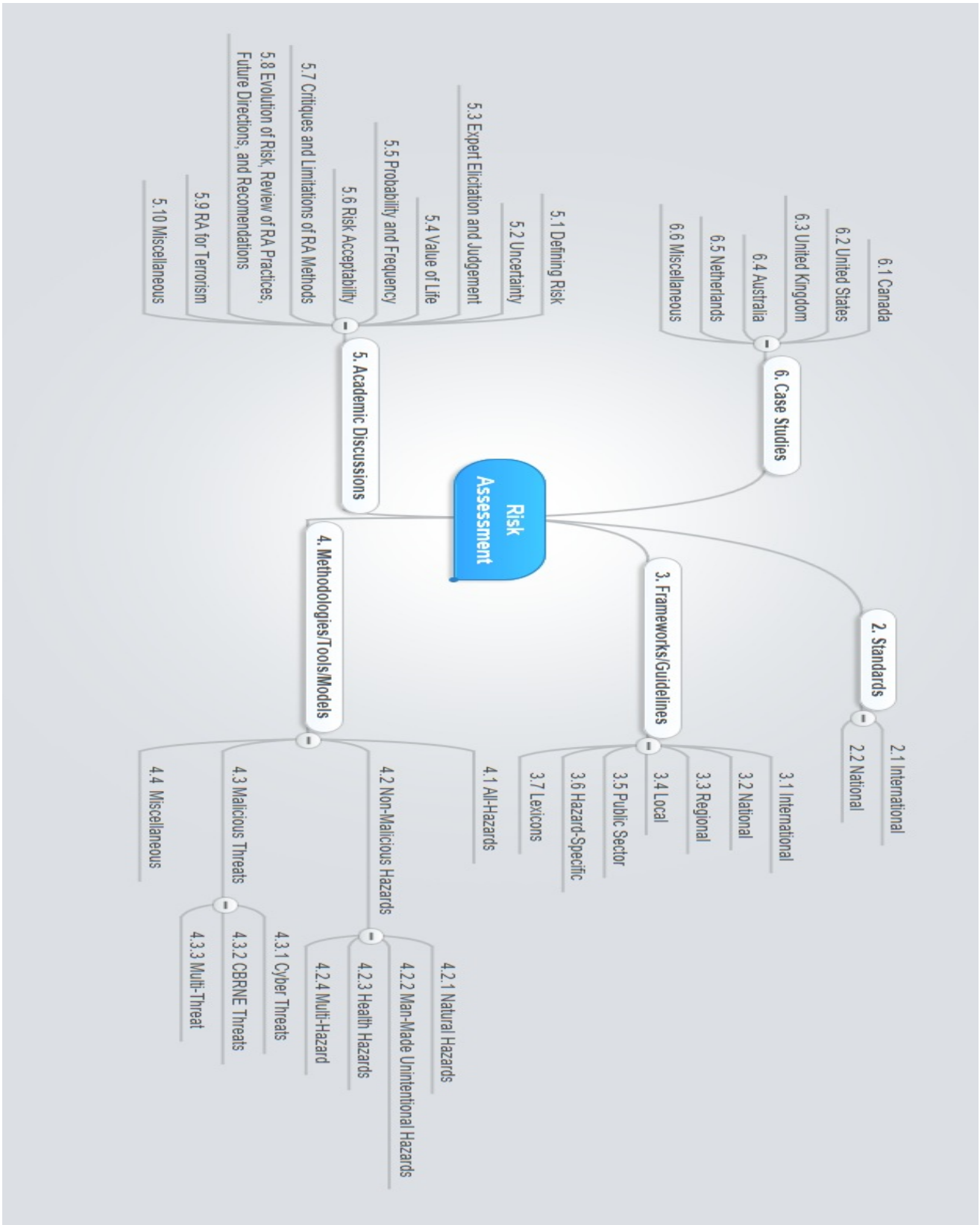

Figure 1- Categorization Scheme

1.5 Document Structure

This document is divided into seven main sections. Introductory material was provided in Section 1. International and national standards are presented in Section 2. Section 3 includes frameworks and guidelines aimed for international, national, regional, local, and public sector use, as well as for specific hazards. Methodologies, tools, and models for all-hazards, non-malicious hazards and malicious threats are presented in Section 4. In Section 5, references on a variety of unique risk-related topics, including critiques of and recommendations for RA practices, are provided. Lastly, a collection of case studies of risk assessments conducted in Canada, the United States, the United Kingdom, Australia, and the Netherlands are presented in section 6, and a summary is provided in Section 7.

2 Standards

Overview

This section presents standards for risk management. A standard is defined as, "a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose." [1]

- **Section 2.1**: international standards, published by the International Organization for Standardization (ISO).
- **Section 2.2**: national standards for Canada and Australia/New Zealand.

Note: Though most of the references in this section are general standards for risk management, one of the standards is specific to information security management.

2.1 International Standards

2.1.1 ISO 31000 Risk Management - Principles and Guidelines

Title: ISO 31000 Risk Management - Principles and Guidelines
Author(s): ISO Technical Management Board Working Group on risk management
Organization: International Organization for Standardization (ISO)
Publisher: Unavailable
Publishing Location: Switzerland
Edition: 1st ed.
Pages: 34
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: November 15, 2009

Objective:

- "It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards." [p. 1]

Scope:

- “This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.
- This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
- This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.” [p. 1]

Description:

- "This International Standard provides principles and generic guidelines on risk management.” [p. 1]
- It includes:
    - Terms and Definitions
    - Description of:
        - Risk Management principles
        - Risk Management framework
        - Risk Management process
    - Annex: Attributes of enhanced risk management

2.1.2 IEC/FDIS 31010: Risk Management - Risk Assessment Techniques

Title: IEC/FDIS 31010: Risk Management - Risk Assessment Techniques
Author(s): Prepared by IEC technical committee 56: Dependability and the ISO TMB "Risk Management" working group
Organization: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Final Draft (2009)
Pages: 92
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: 2009

Scope:

- "This standard is intended to reflect current good practices in selection and utilization of risk assessment techniques, and does not refer to new or evolving concepts which have not reached a satisfactory level of professional consensus. This standard is general in nature, so that it may give guidance across many industries and types of system." [p. 6]

Description:

- "This International Standard is a supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment. The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail." [p. 7]

Additional Information:

- This standard includes:
  - Overview of ISO 31000 Risk management framework
  - Description of ISO 31000 Risk management process
  - Discussion on the selection of techniques, the application of risk assessment during life cycle phases, and the various types of existing techniques
- The annexes provide informative lists and explanations of a range of tools and techniques that can be used to perform or assist with the risk assessment process. They include:
  - Annex A: Comparison of risk assessment techniques
    (Includes a table comparing the applicability of tools used for risk assessment, and a chart comparing the attributes of a selection of risk assessment tools)
  - Annex B: Descriptions on 31 risk assessment techniques
    (For each technique, this annex provides an overview of its use, inputs, process, outputs, strengths and limitations)

2.1.3 ISO/IEC Guide 73: Risk management – Vocabulary – Guidelines for Use in Standards

Title: ISO/IEC Guide 73: Risk management – Vocabulary – Guidelines for Use in Standards
Author(s): ISO Technical Management Board Working Group on risk management terminology
Organization: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC)
Publisher: International Organization for Standardization
Publishing Location: Switzerland
Edition: 1st ed.
Pages: 24
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: 2002

Purpose:

- "The aim of this Guide is to promote a coherent approach to the description of risk management activities and the use of risk management terminology. Its purpose is to contribute towards mutual understanding amongst the members of ISO and IEC rather than provide guidance on risk management practice." [p. 1]

Audience:

- This Guide is aimed at standards writers, and is intended to provide generic definitions in order to support them in preparing or revising standards related to risk management.

Additional Information:
This document includes:

- Terms and definitions
- Diagrams to demonstrate the relationship between terms
- Annex: Terms and Definitions from ISO/IEC Guide 51:1999

2.1.4 BS ISO/IEC 27005: 2011 - Information Technology. Security Techniques. Information Security Risk Management

Title: BS ISO/IEC 27005: 2011 Information technology. Security Techniques. Information Security Risk Management
Author(s): International Organization for Standardization, International Electrotechnical Commission
Organization: International Organization for Standardization, International Electrotechnical Commission
Publisher: BSI
Publishing Location: Unavailable
Edition: 2011 ed., replaces 2008 ed. (2nd ed)
Pages: 50
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: June 2011

Abstract:
"ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011. ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.[2]"

[2] From http://www.iso.org/iso/catalogue_detail?csnumber=56742

2.2 National Standards

2.2.1 CAN/CSA-Q850-97 Risk Management: Guideline for Decision-Makers - A National Standard of Canada

Title: CAN/CSA-Q850-97 Risk Management: Guideline for Decision-Makers - A National Standard of Canada
Author(s): Canadian Standards Association Technical Committee on Risk Management
Organization: Canadian Standards Association
Publisher: Canadian Standards Association
Publishing Location: Etobicoke, ON, CAN
Edition: 1st ed.
Pages: 62
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: 1997, reaffirmed 2007

Purpose:
"The purpose of this Guideline is to provide a comprehensive decision process that will aid decision-makers in identifying, analyzing, evaluating, and controlling all types of risks, including risks to health and safety." [p. 2]

Description:
First, the guideline presents definitions and reference publications. Then, it describes the major steps of the risk management decision process and their relationship to each other. These steps are:

- Initiation
- Preliminary Analysis
- Risk Estimation
- Risk Evaluation
  (Includes a discussion of the ALARA Concept: As Low As Reasonably Achievable)
- Risk Control and Financing
- Action

Additional Information:
The appendices discuss the following topics:

- Uncertainty
- Risk Communication
- Risk Perception and its Effect on the Acceptability of Risk
- Alignment of CSA Guideline CAN/CSA-Q850 to other risk management frameworks

2.2.2 AS/NZS 4360: 2004 Australian/New Zealand Standard: Risk Management

Title: AS/NZS 4360: 2004 Australian/New Zealand Standard: Risk Management
Author(s): Joint Technical Committee OB-007, Risk Management
Organization: Standards Australia, Standards New Zealand
Publisher: Standards Australia International Ltd and Standards New Zealand
Publishing Location: Sydney, AU, and Wellington, NZ
Edition: N/A
Pages: 39
Retrieved from: University of California Office of the President website
Hyperlink: http://www.ucop.edu/riskmgt/erm/documents/as_stdrds4360_2004.pdf
Date of Publication: August 31 2004

Scope:

- "This Standard provides a generic guide for managing risk.
- This Standard may be applied to a very wide range of activities, decisions or operations of any public, private or community enterprise, group or individual…
- It is generic and independent of any specific industry or economic sector…
- This Standard should be applied at all stages in the life cycle of an activity, function, project, product, or asset…
- The process described here applies to the management of both potential gains and potential losses." [p. 1]

Additional Information:
This document includes:

- Definitions
- Description of the risk management process:
    - Communicate and consult
    - Establish the context
    - Identify risks
    - Analyse risks
    - Evaluate risks
    - Treat risks
    - Monitor and review
    - Record the risk management process
- Explanation on how to establish effective risk management in an organization

3 Frameworks and Guidelines

Overview

This section presents frameworks and guidelines for risk assessment and risk management. These references are divided into sub-sections according to their intended use.

- **Section 3.1**: a framework for international risk governance.
- **Section 3.2**: a framework for a national risk assessment.
- **Section 3.3**: a guideline for regional risk assessments.
- **Section 3.4**: frameworks and guidelines for local risk assessment and management.
- **Section 3.5**: frameworks and guidelines for risk management in public sector organizations.
- **Section 3.6**: frameworks and guidelines for risk assessment and management for specific hazards.
- **Section 3.7**: lexicons of key risk-related terms.

Note: Some of the references included in this section may not be frameworks or guidelines per se, but were included because they describe general principles, foundational ideas, or definitions, all of which contribute to the formulation of risk frameworks.

3.1 International

3.1.1 Risk Governance: Towards an Integrative Approach

Title: Risk Governance: Towards an Integrative Approach
Author(s): Ortwin Renn with Annexes by Peter Graham
Organization: International Risk Governance Council (IRGC)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 156
Retrieved from: International Risk Governance Council, White Paper no. 1
Hyperlink: N/A
Date of Publication: September 2005

Purpose:

- "This document aims to guide the work of the International Risk Governance Council and its various bodies in devising comprehensive and transparent approaches to 'govern' a variety of globally relevant risks." [p. 17]

Audience:

- This document is intended for use by the International Risk Governance Council (IRGC). In addition, it has the potential to be of use to senior risk managers and decision makers, as well as risk practitioners external to the IRGC.

Description:

- This paper presents an "integrated analytic framework for risk governance which provides guidance for the development of comprehensive assessment and management strategies to cope with risks, in particular at the global level. The framework integrates scientific, economic, social and cultural aspects and includes the effective engagement of stakeholders. The framework reflects IRGC's [International Risk Governance Council] own priorities: improvement of risk governance strategies for risks with international implications and which have the potential to harm human health and safety, the economy, the environment, and/or the fabric of society at large." [p. 11]

Additional Information:
This framework offers two innovative contributions to the risk field. They are:

- Inclusion of the societal context
- Categorisation of risk-related knowledge based on the varying states of knowledge about each risk (simple, complex, uncertain and ambiguous risk problems)

3.2 National

3.2.1 A National Risk Assessment Framework for Sudden Onset Hazards

Title: A National Risk Assessment Framework for Sudden Onset Hazards
Author(s): Unavailable
Organization: Australian Emergency Management Committee
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Version 2.6
Pages: 24
Retrieved from: Asia Pacific Gateway for Disaster Risk Reduction and Development website
Hyperlink: http://www.drrgateway.net/sites/default/files/australia_risk_assessment_framework.pdf
Date of Publication: June 27, 2007

Purpose:

- "This framework is designed to improve our collective knowledge about natural hazard risk in Australia to support emergency risk management and natural hazard mitigation." [p. 4]
- "This framework will lead to a broader and more systematic approach to risk assessment that explicitly involves all levels of government (Australian, State, Territory and Local) and which has the aims of improving risk management outcomes." [p. 5]

Scope:

- "The natural hazards covered are those defined in the report to the COAG [Council of Australian Governments]: bushfire, earthquake, flood, storm, cyclone, storm surge, landslide, tsunami, meteorite strike and tornado...
- This framework focuses on risk assessment for sudden onset natural hazards to underpin natural hazard risk management and natural hazard mitigation. The framework does not focus on risk management or mitigation, although its outcomes support and benefit these.
- The framework covers the following risks arising from natural hazards: financial, socio-economic, casualty, political and environmental risk. Each of these risks contributes to the overall impacts of natural hazards on communities." [p. 4]

Audience:

- "This framework is aimed foremost at those who seek an improved evidence base for risk management of natural hazards, in all levels of government. The framework is also intended for risk assessment practitioners, researchers and information managers." [p. 4]

Description:
This document establishes a framework by describing:

- Roles in the framework
- How to produce baseline information and improve risk assessment methods
- How to manage and access information on risk

3.3 Regional

3.3.1 Getting it Right: Assessing and Building Resilience in Canada's North

Title: Getting it Right: Assessing and Building Resilience in Canada's North
Author(s): Stefan Fournier
Organization: Conference Board of Canada
Publisher: Unavailable
Publishing Location: Canada
Edition: Unavailable
Pages: 66
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: May 2012

Description:

- "This report provides policy-makers, emergency management practitioners, and community and business leaders with a conceptual understanding of community resilience and what it means for Canada's Northern communities. It also provides guidance on how to approach risk and resilience assessment methods and models to assess and enhance the resilience of Northern communities. The report identifies existing links between the concept of community security, as defined by Northerners, and the elements that are essential for enhancing community resilience. It then establishes the distinct risk context facing Northern communities by identifying some of the key strengths and sources of their resilience, as well as sources of risk that challenge this resilience. Finally, the report looks at a range of current risk and resilience assessment tools, and sets out four guiding principles that are essential for an effective Northern assessment process." [Preface]

Additional Information:

- Chapter 4 of this report is dedicated to risk and resilience assessment models and initiatives. This chapter presents an overview of select assessment models and measurement initiatives, as well as a comparative analysis of their strengths and weaknesses.

3.4 Local

3.4.1 Disaster Resilience by Design: A Framework for Integrated Assessment and Risk-Based Planning in Canada

Title: Disaster Resilience by Design: A Framework for Integrated Assessment and Risk-Based Planning in Canada
Author(s): Murray Journeay with research contributions by Sonia Talwar, Boyan Brodaric and Nicky Hastings
Organization: Earth Sciences Sector of Natural Resources Canada, in collaboration with the Canadian Institute of Planners, with support from the CRTI Program of Defence Research and Development Canada
Publisher: Unavailable
Publishing Location: Canada
Edition: Draft Version 1.0
Pages: 336
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: June 2011

Objectives:

- "To research best practices for the assessment of natural hazard risks at local and regional scales in Canada;
- To design and build a framework for integrated risk assessment and scenario-based planning that is standards-based and that can be implemented using available methods and tools; and
- To evaluate the efficacy of the proposed framework through case-based research with agencies that are actively involved in disaster mitigation activities on the ground." [p. 16]

Audience:

- “Outputs of this study will be of particular interest to domain experts and practitioners involved in risk-based planning at the scale of individual communities and regions, and to those working toward the development of a broader framework for disaster risk reduction in Canada.” [p. 19]

Description:

- This document is the "result of a five-year research and development effort by the Earth Sciences Sector of Natural Resources Canada (ESS/NRCan). The study explores the realm of disaster risk reduction in North America, and introduces a framework for integrated assessment and scenario planning to assist local and regional governments in managing the risks associated with growth and development in areas exposed to natural hazards." [p. 4]

Additional Information:

- “Part 1 establishes overall context and focus for disaster risk reduction in the public domain, and introduces an earth systems approach to risk-based planning that is rooted in theoretical principles and best practices of risk analysis, integrated assessment, and scenario modelling (Chapter 1, 2, and 3).
- Part 2 introduces an integrated framework of processes, methods and tools (Pathways) that has been developed to guide risk-based planning at local and regional scales (Chapter 4). It also documents the results of an interactive case study project in which elements of the Pathways framework were tested and evaluated in support of a comprehensive risk-based planning process in southwest British Columbia, Canada (Chapter 5)." [p. 19]

3.4.2 Emergency Preparedness: Guidance on Part 1 of the Civil Contingencies Act 2004, its Associated Regulations and Non-Statutory Arrangements

Title: Emergency Preparedness: Guidance on Part 1 of the Civil Contingencies Act 2004, its Associated Regulations and Non-Statutory Arrangements
Author(s): Her Majesty's (HM) Government
Organization: HM Government
Publisher: HM Government
Publishing Location: United Kingdom
Edition: Unavailable
Pages: 232
Retrieved from: National Archives, UK Government website
Hyperlink:
http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/131903/emergprepfinal.pdf
Date of Publication: 2004

Description:

- This guide "sets out the generic framework for civil protection. As such, it deals with pre-emergency elements of integrated emergency management – anticipation, assessment, prevention and preparation." [p. 3]
- This guide describes the requirements of Part 1 of the Civil Contingencies Act of 2004, and provides guidance on how various bodies can carry out their duties to comply with the legislation. Special attention is given to bodies at the local level.

Additional Information:
Chapter 4 and its annexes are specific to risk assessment:

- Chapter 4: Local Responder Risk Assessment
  Pg. 34-46
  Describes and recommends a six-step risk assessment process
- Annex 4A: Summary of the six-step local risk assessment process
  Pg. 183-185
- Annex 4B: Illustration of a Local Risk Assessment Guidance (LRAG)
  Pg. 186-192
- Annex 4C: Example of an individual risk assessment
  Pg. 193-194
- Annex 4D: Likelihood and impact scoring scales
  Pg. 195-197
- Annex 4E: Community Risk Register
  Pg.198
- Annex 4F: Risk Rating Matrix
  Pg. 199-200

3.4.3 Working Together to Protect Crowded Places

Title: Working Together to Protect Crowded Places
Author(s): Her Majesty's (HM) Government
Organization: HM Government
Publisher: HM Government
Publishing Location: United Kingdom
Edition: Unavailable
Pages: 38
Retrieved from: National Counter Terrorism Security Office
Hyperlink: https://vsat.nactso.gov.uk/SiteCollectionDocuments/AreasOfRisk/working-together-crowded-places.pdf
Date of Publication: March 2010

Scope:
- Crowded places, excluding buildings in the transport sector or schools

Audience:
- This guidance aims to "help local authorities, the police, members of Crime and Disorder Reduction Partnerships and Local Resilience Forums, Community Safety Partnerships in Wales, Strategic Coordinating Groups in Scotland, as well as other local partners, including businesses, understand their role and the contributions they can make to reduce the vulnerability of crowded places to terrorist attack." [p. 7]

Description:
- "This guidance describes the key principles that inform our work to improve the protective security of crowded places, the contributions that a wide range of partners can make and how vulnerabilities can best be reduced." [p. 5]
- "In particular, it explains:
  - how risk will be assessed and local performance managed; and
  - the roles of key partners in helping to reduce the vulnerability of crowded places to terrorist attack." [p. 7]

Additional Information:
This document is structured as follows:
- Key principles
- Roles and responsibilities
- Reducing the vulnerability of crowded places
  - Describes the work of Counter-Terrorism Security Advisors (CTSAs) to assess the vulnerability of crowded places as well as the actions that local stakeholders must take
  - Describes a vulnerability self-assessment tool
- Reducing Vulnerabilities: What Works?
- Annexes:
  - Crowded places risk assessment matrix
  - Information exchange between national and local stakeholders

3.4.4 Emergency Risk Management Applications Guide

Title: Emergency Risk Management Applications Guide
Author(s): Emergency Management Australia
Organization: Emergency Management Australia
Publisher: Emergency Management Australia
Publishing Location: Australia
Edition: 2nd ed.
Pages: 68
Retrieved from: Australian Emergency Manuals Series, Manual 5
Hyperlink: http://www.em.gov.au/Documents/Manual%2005-ApplicationsGuide.pdf
Date of Publication: 2004

Purpose:

- “The purpose is to provide a generic overview of the ERM process.” [p. 9]

Scope:

- "Encompasses major risks to community safety that require whole-of-community or multi-organisational attention." [p. 10]

Audience:

- "People in communities and government organizations (at all levels) who are involved in emergency risk management." [p. 10]

Description:

- This document provides step-by-step guidance through the Emergency Risk Management process. For each step, the guide provides supplementary examples, criteria, or references.

Additional Information:
This Guide also describes and recommends the following emergency risk management tools:

- Unique identifier system
- Risk register database
- Geographic information systems

3.4.5 Model Community Emergency Risk Management Plan (Part A - Guidelines)

Title: Model Community Emergency Risk Management Plan (Part A - Guidelines)
Author(s): Local Government Association (LGA) of South Australia, Australian Government
Organization: Local Government Association (LGA) of South Australia, Australian Government
Publisher: Local Government Association (LGA) of South Australia, Australian Government
Publishing Location: Unavailable
Edition: Unavailable
Pages: 39
Retrieved from: Local Government Association of South Australia website
Hyperlink: http://www.lga.sa.gov.au/webdata/resources/files/Part_A_Guidelines_-_Model_Community_Emergency_Risk_Management_Plan.PDF
Date of Publication: June 2008

Purpose:

- "These Model Community Emergency Risk Management plans (CERM) were developed to provide guidance and promote best practice emergency planning for South Australian Local Government." [p. 3]

Scope:

- These Guidelines were created for the South Australian context. Thus, the Guidelines are not directly transferable to other jurisdictions.

Description:

- These Guidelines provide "context and assistance for Councils in developing, or updating, a CERM using a risk management approach." [p. 4]
- This document provides guidance through each of the steps involved in creating a Community Emergency Risk Management plan. The steps are:
  1. Establishing the Community Emergency Risk Management (CERM) Project
  2. Establishing the Context
  3. Risk Assessment
  4. Risk Treatment

Additional Information:

- The guidelines also include criteria, a risk assessment register, planning tables, and supplementary annexes in order to assist users throughout the process.

3.4.6 Community Emergency Risk Management Plan (Part B - Template)

Title: Community Emergency Risk Management Plan (Part B - Template)
Author(s): Local Government Association (LGA) of South Australia, Australian Government
Organization: Local Government Association (LGA) of South Australia, Australian Government
Publisher: Local Government Association (LGA) of South Australia, Australian Government
Publishing Location: Unavailable
Edition: 1.0 Initial framework
Pages: 36
Retrieved from: Local Government Association of South Australia website
Hyperlink: N/A
Date of Publication: 2008

Description:
This document is a supplement to the Model Community Emergency Risk Management (CERM) Plan (Part A – Guidelines). Part B of the CERM plan is a template which can be filled in with information specific to a community or region. This template provides assistance through each of the four steps involved in creating a CERM plan.

3.5 Public Sector

3.5.1 Framework for the Management of Risk

Title: Framework for the Management of Risk
Author(s): Treasury Board of Canada Secretariat
Organization: Treasury Board of Canada Secretariat
Publisher: Treasury Board of Canada Secretariat
Publishing Location: Canada
Edition: 2010 version
Pages: N/A
Retrieved from: Treasury Board of Canada Secretariat website
Hyperlink: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text
Date of Publication: 2010

Purpose:

- "The purpose of this Framework is to provide guidance to Deputy Heads on the implementation of effective risk management practices at all levels of their organization. This will support strategic priority setting and resource allocation, informed decisions with respect to risk tolerance, and improved results.[3]"

Description:

- This Framework outlines the roles and responsibilities of Deputy Heads, the Treasury Board, and the Treasury Board of Canada Secretariat with respect to risk management.

[3] From http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text

3.5.2 Guide to Integrated Risk Management

Title: Guide to Integrated Risk Management
Author(s): Treasury Board of Canada Secretariat
Organization: Treasury Board of Canada Secretariat
Publisher: Treasury Board of Canada Secretariat
Publishing Location: Canada
Edition: 2010 version
Pages: N/A
Retrieved from: Treasury Board of Canada Secretariat website
Hyperlink: http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-eng.asp
Date of Publication: 2010

Purpose:

- "This Guide is intended to help strengthen Canadian federal public sector integrated risk management practices by providing organizations with guidance in the design, implementation, conduct and continuous improvement of integrated risk management that will result in a risk-informed approach to management throughout the organization ultimately leading to better performance.[4]"

Description:

- "This Guide is intended as a companion document to the principles-based TBS *Framework for the Management of Risk* (2010). It elaborates on the principles in the *Framework* and provides practical guidance and considerations for operationalizing these principles as part of an organization's integrated risk management strategy. It also provides information about linkages to some generic risk management resources such as processes, practices, tools and templates that may be adapted to the circumstances of specific federal organizations, depending on their size, mandate, organizational structure and lines of business.[5]"

Additional Information:

- This Guide provides an overview of the TBS Framework for the Management of Risk, including key concepts, risk management principles, as well as the roles and responsibilities of deputy heads and the Treasury Board of Canada Secretariat.
- The Guide also offers descriptions of the key elements of the risk management process. They are:
    - "Planning and Designing the Approach and Process (Getting started)
    - Implementing Integrated Risk Management (Putting it in place)
    - Practicing Integrated Risk Management (Doing it)
    - Continuously Improving Integrated Risk Management (Improving it)"[6]

[4] From http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-eng.asp
[5] Ibid.
[6] http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir02-eng.asp

3.5.3 Integrated Risk Management Framework

Title: Integrated Risk Management Framework
Author(s): Treasury Board of Canada Secretariat
Organization: Treasury Board of Canada Secretariat
Publisher: Treasury Board of Canada Secretariat
Publishing Location: Canada
Edition: 2001 version
Pages: 21
Retrieved from: Treasury Board website
Hyperlink: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254
Date of Publication: 2001
*Replaced by the Framework for the Management of Risk (2010)

Purpose:

- "The Framework provides an organization with a mechanism to develop an overall approach to manage strategic risks by creating the means to discuss, compare and evaluate substantially different risks on the same page.[7]"

Scope:

- The Framework "applies to an entire organization and covers all types of risks faced by that organization (e.g. policy, operational, human resources, financial, legal, health and safety, environment, reputational).[8]"

Description:
This framework offers:

- A description of three key concepts: risk, risk management, and integrated risk management
- An overview of the Integrated Risk Management Framework, description of its four elements, and a synopsis of the expected results

Additional Information:
The Four Elements of the Integrated Risk Management Framework are:

- "Developing the Corporate Risk Profile…
- Establishing an Integrated Risk Management Function…
- Practising Integrated Risk Management…
- Ensuring Continuous Risk Management Learning[9]"

[7] From http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254
[8] Ibid.
[9] Ibid.

3.5.4 Integrated Risk Management - Implementation Guide

Title: Integrated Risk Management - Implementation Guide
Author(s): Treasury Board of Canada Secretariat
Organization: Treasury Board of Canada Secretariat
Publisher: Treasury Board of Canada Secretariat
Publishing Location: Canada
Edition: 2004 version
Pages: 102
Retrieved from: Treasury Board of Canada Secretariat website
Hyperlink: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide-eng.asp
Date of Publication: 2004
*Replaced by the Guide to Integrated Risk Management (2010)

Scope:

- "The guide's focus is integrated risk management, not risk management.[10]"

Description:

- "This guide is a companion to the Government of Canada's Integrated Risk Management Framework (IRMF) of April 2001. It is intended for use with the IRMF in implementing integrated risk management in a federal organization.[11]"
- "This guide provides practical advice to those leading and facilitating implementation of integrated risk management in their organizations. It will be useful as well in increasing understanding and collaboration where needed. Risk champions familiar with the IRMF can look to the guide for what to do next. The guide is also a reference tool for assessing progress and identifying gaps in organizations where integrated risk management is already underway.[12]"

Additional Information:

- After presenting some introductory material and tips for getting started, this guide breaks down into 4 sections, which reflect the four elements of the Integrated Risk Management Framework. They are:
  1. "Developing the Corporate Risk Profile;
  2. Establishing an Integrated Risk Management Function—Integrating Risk Management into Existing Decision–making Processes and Reporting;
  3. Practising Integrated Risk Management; and
  4. Ensuring Continuous Risk Management Learning.[13]"
- For each of the elements above, the guide discusses the fundamentals, how to do it, questions to consider, and provides examples.
- "Also at the end of the guide is an overview chart summarizing the steps in implementing an integrated approach to risk management within an organization. It describes key requirements and decisions for the critical stages in the process. Following the overview are summaries of what and how for establishing each IRMF element—practices and techniques for what organizations have done or need to do to develop and implement the particular element.[14]"

[10] From http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide02-eng.asp
[11] From http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide01-eng.asp
[12] From http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide02-eng.asp
[13] From http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide01-eng.asp
[14] From http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide02-eng.asp

3.5.5 A Primer on Risk Management in the Public Service

Title: A Primer on Risk Management in the Public Service
Author(s): Stephen Hill (University of Calgary)
Organization: Canadian Centre for Management Development (CCMD)
Publisher: Unavailable
Publishing Location: Canada
Edition: Unavailable
Pages: 17
Retrieved from: A background document for CCMD's Action-Research Roundtable on Risk Management, from the Canada School of Public Service website
Hyperlink: http://www.csps-efpc.gc.ca/pbp/pub/pdfs/W11_e.pdf
Date of Publication: 2001

Purpose:

- "This primer is not meant to be an exhaustive review or treatment of risk management. Rather, the intent is to create a common point of departure for learning and work on what constitutes good risk management and what obstacles might be encountered in incorporating risk management into government decision making." [p. 3]

Description:
This primer briefly reviews some of the basic concepts of risk management, particularly as they apply to the public service. The concepts covered are:

- What is risk
- Managing Risks?
- Risk Management Frameworks
- Identifying Risks
- Assessment of Risk
- Responding to and Managing Risk
- Monitoring Effectiveness: Feedback and Learning

3.5.6 A Foundation for Developing Risk Management Learning Strategies in the Public Service

Title: A Foundation for Developing Risk Management Learning Strategies in the Public Service
Author(s): Canadian Centre for Management Development (CCMD) Roundtable on Risk Management
Organization: Canadian Centre for Management Development
Publisher: Canadian Centre for Management Development
Publishing Location: Canada
Edition: Unavailable
Pages: 49
Retrieved from: Canada School of Public Service website
Hyperlink: http://www.csps-efpc.gc.ca/pbp/pub/pdfs/P100_e.pdf
Date of Publication: 2001

Purpose:

- "The intent of this document is to provide a foundation for developing learning strategies and curriculum for public sector risk management…This document does not provide the specific content for a course on risk management, which should necessarily be context specific. Rather, it attempts to set broad curriculum goals that will provide the foundation for course and training development both by CCMD [Canadian Centre for Management Development] and within specific departments." [p. v]

Scope:

- This document focuses on the "cultural challenges of building organizations that make sound, public-interest decisions in the midst of uncertainty." [p. vi]

Audience:

- Risk managers in the public sector

Additional Information:
This document includes:

- An overview of risk management concepts
- The learning requirements for effective risk management in the public service
- Recommendations for the foundations of a risk management curriculum for the public service

3.5.7 Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management

Title: Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management
Author(s): ADM Working Group on Risk Management
Organization: Privy Council Office
Publisher: Unavailable
Publishing Location: Canada
Edition: Unavailable
Pages: 30
Retrieved from: Privy Council Office website
Hyperlink: http://www.pco-bcp.gc.ca/docs/information/publications/aarchives/social-dev/risk-management-eng.pdf
Date of Publication: March 2000

Purpose:

- "This report addresses the issue of risk management in the context of public policy by:
  - Highlighting the fact that risk management concepts apply broadly throughout government;
  - Serving as a resource for departments and agencies to help stimulate debate about the nature of risk in their sectors, and about the appropriate processes and capabilities for managing such risks;
  - Providing initial findings and recommendations on broad, overarching issues in risk management with relevance throughout government; and,
  - Tasking key departments and agencies with leadership roles to help advance risk management in priority areas." [p. 1]

Description:

- "The report first examines various criteria required to launch a discussion, i.e. terminology issues and risk concepts. It then presents a framework, created to integrate various key concepts and to provide a platform for discussing risk management from a wide range of public policy perspectives.
- As a summary, the report makes recommendations for raising awareness of risk management as a public policy issue and for advancing the discussion of certain key issues." [p. 1]

3.5.8 Risk Management Guideline for the BC Public Sector

Title: Risk Management Guideline for the BC Public Sector
Author(s): Province of British Columbia Risk Management Branch and Government Security Office
Organization: Province of British Columbia Risk Management Branch and Government Security Office
Publisher: Province of British Columbia
Publishing Location: British Columbia, Canada
Edition: Unavailable
Pages: 22
Retrieved from: British Columbia Government website
Hyperlink: http://www.fin.gov.bc.ca/pt/rmb/ref/RMB_ERM_Guideline.pdf
Date of Publication: March 28, 2012

Scope:

- This document "guides the application of risk management within ministries, central agencies and service crowns. Commercial Crowns…and other members of the wider public sector such as health authorities and school districts are encouraged to review this guideline and apply the contents as appropriate." [p. 4]

Audience:

- "This guideline serves primarily BC government ministry and provincial public sector employees having risk management responsibilities. It is also a useful reference for those wishing to incorporate the risk management process into business planning, project management, procurement, service delivery and policy development." [p. 4]

Description:

- "This guideline and the companion *CAN/CSA ISO 31000: Risk Management - Principles and Guidelines* provides the direction and process for standardizing the risk management practice in the Province." [p. 2]

Additional Information:
This publication includes guidance on:

- BC Risk Management
  - Provincial Risk Management Framework
  - Roles and Responsibilities
  - Policy
  - Additional Information
- Application of the Risk Management Process
  - General
  - Communicate and Consult
  - Establish the Context
  - Identify Risk
  - Analyze Risk
  - Evaluate Risk: Existing Controls, Tolerance and Action
  - Treat Risk
  - Monitor and Review
  - Record the Risk Management process

  (This section includes examples and rating charts to assist readers through the risk management process.)

3.5.9 Risk Management Fundamentals - Homeland Security Risk Management Doctrine

Title: Risk Management Fundamentals - Homeland Security Risk Management Doctrine
Author(s): Office of Risk Management and Analysis, Department of Homeland Security (DHS)
Organization: Department of Homeland Security (DHS)
Publisher: Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: Unavailable
Pages: 31
Retrieved from: Department of Homeland Security website
Hyperlink: http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf
Date of Publication: April 2011

Objectives:

- "This doctrine, *Risk Management Fundamentals*, serves as an authoritative statement regarding the principles and process of homeland security risk management and what they mean to homeland security planning and execution. It is intended as the capstone doctrine on risk management for the Department of Homeland Security (DHS). Furthermore, Risk Management Fundamentals serves as a foundational document supporting DHS risk management efforts in partnership with the homeland security enterprise.
- *Risk Management Fundamentals* is intended to help homeland security leaders, supporting staffs, program managers, analysts, and operational personnel develop a framework to make risk management an integral part of planning, preparing, and executing organizational missions. The development of homeland security risk management doctrine is an essential element in promoting a risk-informed culture enabling training, capability development, and integration across DHS to strengthen and improve the Nation's security. *Risk Management Fundamentals* articulates a desired end-state that DHS aspires to achieve in promoting risk management." [p. 5]

Audience:

- Primarily DHS employees.
- However, this document may also be helpful to Federal interagency partners, state and local agencies, as well as the larger homeland security community.

Additional Information:
This document includes information on:

- Homeland Security Risk Management Tenets and Principles
- A Comprehensive Approach to Risk Management
- The Homeland Security Risk Management Process

3.5.10 The Orange Book: Management of Risk - Principles and Concepts

Title: The Orange Book: Management of Risk - Principles and Concepts
Author(s): HM (Her Majesty's) Treasury
Organization: HM (Her Majesty's) Treasury
Publisher: HM (Her Majesty's) Treasury
Publishing Location: United Kingdom
Edition: Unavailable
Pages: 52
Retrieved from: HM Treasury website (UK)
Hyperlink: http://www.hm-treasury.gov.uk/d/orange_book.pdf
Date of Publication: October 2004

Purpose:

- "This guide aims to provide an introduction to the range of considerations which apply in risk management, all of which can be applied at various levels ranging from the development of a strategic, organization-wide risk policy through to management of a particular project or operation. It does so using a risk management model...
- The guide focuses firstly on the "lifecycle" core of the model, then gives consideration to the wider based issues which form the overall risk management environment.
- It is important to note that this guide is *not* a detailed instruction manual for how to manage risk - its aim is simply to draw attention to the range of issues which are involved and to offer some general direction to help the reader think about how these issues may be addressed in the specific circumstances of their own organization." [p. 10]

Description:

- This publication is a successor to the 2001 *Management of Risk - A Strategic Overview*, which became a valuable resource for developing and implementing risk management processes in government organizations. Since most government organizations now have basic risk management processes in place, *The Orange Book: Management of Risk - Principles and Concepts* includes a stronger focus on the ongoing improvement of risk management.

Additional Information:

- This guide discusses the issues and concepts involved in each step of the risk management model. The components are:
  - Identifying risks
  - Assessing risks
  - Addressing risks
  - Reviewing and reporting risks
  - Communication and learning
  - The extended enterprise
  - Risk environment and context
- The guide also includes:
  - A discussion on risk appetite
  - An example on how to document risk assessment
  - Overall assurance on risk management
  - Summary of horizon scanning issues

3.6 Hazard/Threat -Specific

3.6.1 WHO SARS Risk Assessment and Preparedness Framework

Title: WHO SARS Risk Assessment and Preparedness Framework
Author(s): Department of Communicable Disease Surveillance and Response, World Health Organization (WHO)
Organization: Department of Communicable Disease Surveillance and Response, World Health Organization (WHO)
Publisher: World Health Organization (WHO)
Publishing Location: Unavailable
Edition: Unavailable
Pages: 33
Retrieved from: World Health Organization website
Hyperlink: http://www.who.int/csr/resources/publications/CDS_CSR_ARO_2004_2.pdf
Date of Publication: October 2004

Description:

- "This document sets out a framework of activities, at national and international levels, that can be used to assess the risk that SARS might recur and to prepare appropriate contingency plans. Modelled on WHO's influenza pandemic preparedness plan, the framework adopts a phased approach in which recommended activities escalate in line with the evolving epidemiological situation. Phases are defined by distinct epidemiological criteria, such as the detection of sporadic cases with no secondary spread, the establishment of human-to-human transmission, and evidence of international spread. The possibility that the SARS coronavirus might behave differently than during the 2002–2003 international outbreak is also taken into account." [p. 3]

Additional Information:

- The framework is organized according to six phases. They are:
    - Inter-epidemic period: No evidence of SARS - CoV transmission to humans worldwide
    - Inter-epidemic period: Sporadic case(s) of SARS
    - Confirmed human-to-human transmission
    - International Spread of SARS
    - Slowing down of the outbreak
    - Global interruption of SARS-CoV transmission (epidemic halted)
- For each of the above phases, this framework describes a range of activities for countries/areas with reported SARS cases and for those free of SARS. In addition, the framework includes those activities that will be undertaken by WHO, as well as the types of assistance that WHO can provide to countries. These lists of activities should support the creation of contingency plans.

3.6.2 A Guide to Health Risk Assessment

Title: A Guide to Health Risk Assessment
Author(s): California Environmental Protection Agency, Office of Environmental Health Hazard Assessment
Organization: California Environmental Protection Agency, Office of Environmental Health Hazard Assessment
Publisher: Office of Environmental Health Hazard Assessment
Publishing Location: California, United States of America
Edition: Unavailable
Pages: 12
Retrieved from: Office of Environmental Health Hazard Assessment website
Hyperlink: http://oehha.ca.gov/pdf/HRSguide2001.pdf
Date of Publication: Unavailable

Purpose:

- "The purpose of this booklet is to provide a basic explanation of risk assessment for laypeople involved in environmental health issues, including policymakers, businesspeople, members of community groups, news reporters, and others with an interest in the potential health effects of toxic chemicals." [p. 2]

Description:

- This booklet very briefly describes a four-step risk assessment process: hazard identification, exposure assessment, dose-response assessment, and risk characterization. It also provides a brief explanation about how risk assessment is used by risk managers.

3.6.3 Are We Forgetting the Risks of Information Technology?

Title: Are We Forgetting the Risks of Information Technology?
Author(s): Thomas A. Longstaff, Clyde Chittister, Rich Pethia, Yacov Y. Haimes
Organization: Institute of Electrical and Electronics Engineers (IEEE)
Publisher: IEEE Computer Society Press
Publishing Location: Los Alamitos, CA
Edition: N/A
Pages: 43-51
Retrieved from: Computer, Vol. 33, Issue 12
Hyperlink: N/A
Date of Publication: December 2000

Abstract:
"The emerging dominance of software in the lifecycle of our information systems, coupled with the risk and uncertainty associated with its development and maintenance, are increasing information systems vulnerability. Global interconnected-ness through the Internet and the increasing use of supervisory control and data acquisition systems to remotely operate the critical infrastructure through the telecommunications network have rendered our information systems more vulnerable to intrusion and the transmission of malicious misinformation and signals. For all practical purposes, international boundaries have been eliminated in cyber-space. The growth of information technology and almost universal access to computers have enabled hackers and would-be terrorists to attack information systems and critical infrastructures worldwide. The authors describe the hierarchical holographic modeling framework, which promotes a systemic process for assessing risk to critical infrastructures.[15]"

[15] From http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=889092&tag=1

3.6.4 Measuring the Risk-Based Value of IT Security Solutions

Title: Measuring the Risk-Based Value of IT Security Solutions
Author(s): Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang
Organization: N/A
Publisher: Institute of Electrical and Electronics Engineers (IEEE) Computer Society
Publishing Location: Unavailable
Edition: N/A
Pages: 35-42
Retrieved from: IT Professional, Vol. 6, Issue 6
Hyperlink: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1390871
Date of Publication: Nov-Dec. 2004

Abstract:
"Information security problems cost millions of dollars for US companies and billions for the overall US economy. Nowadays, the question is not whether organizations need more security, but how much to spend for added security. And yet investing in IT security has always been a hard sell for IT managers. Scores of security technologies are on the market and, if anything is certain, it is that none of them can guarantee security. Each choice involves risk. The problem is that security managers lack structured cost-benefit methods to evaluate IT security solutions in light of prevailing uncertainties. A framework can help evaluate the costs and benefits of IT security solutions using a company's risk profile. Using an unconventional concept, this framework bases benefit on avoided risk rather than increased productivity. Lawrence Berkeley National Laboratory (LBNL) uses this framework to help demonstrate to management and auditors that it is significantly less expensive to accept some damage from cyberattacks than to attempt to prevent all possible damages. This pragmatic approach continues to enable LBNL's cybersecurity staff to optimize security countermeasure investments and reduce spending without sacrificing protection. The framework described here uses a risk management approach that integrates risk profile with actual damages and implementation costs to determine the costs and benefits of information security solutions. This approach requires reasonably voluminous data and is thus well suited for organizations with extensive incident data or when the consequences of incidents are high enough to warrant extensive data gathering." [p. 35]

3.6.5 Assessing Risk from Intelligent Attacks: A Perspective on Approaches

Title: Assessing Risk from Intelligent Attacks: A Perspective on Approaches
Author(s): Seth D. Guikema, Terje Aven
Organization: N/A
Publisher: Elsevier Ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 478-483
Retrieved from: Reliability Engineering and System Safety, Vol. 95, No. 5
Hyperlink: N/A
Date of Publication: May 2010

Abstract:
"Assessing the uncertainties in and severity of the consequences of intelligent attacks are fundamentally different from risk assessment for accidental events and other phenomena with inherently random failures. Intelligent attacks against a system involve adaptation on the part of the adversary. The probabilities of the initiating events depend on the risk management actions taken, and they may be more difficult to assess due to high degrees of epistemic uncertainty about the motivations and future actions of adversaries. Several fundamentally different frameworks have been proposed for assessing risk from intelligent attacks. These include basing risk assessment and management on game theoretic modelling of attacker actions, using a probabilistic risk analysis (PRA) approach based on eliciting probabilities of different initiating events from appropriate experts, assessing uncertainties beyond probabilities and expected values, and ignoring the probabilities of the attacks and choosing to protect highest valued targets. In this paper we discuss and compare the fundamental assumptions that underlie each of these approaches. We then suggest a new framework that makes the fundamental assumptions underlying the approaches clear to decision makers and presents them with a suite of results from conditional risk analysis methods. Each of the conditional methods presents the risk from a specified set of fundamental assumptions, allowing the decision maker to see the impacts of these assumptions on the risk management strategies considered and to weight the different conditional results with their assessments of the relative likelihood of the different sets of assumptions." [p. 478]

3.6.6 Terrorism Threat Assessment and Management

Title: Terrorism Threat Assessment and Management
Author(s): Gordon Woo, Risk Management Solutions, London UK
Organization: Center of Excellence - Defence Against Terrorism
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages:101-116
Retrieved from: Defence Against Terrorism Review, Vol. 2, No. 1
Hyperlink: http://www.tmmm.tsk.tr/publications/datr3/06_Gordon%20Woo.pdf
Date of Publication: Spring 2009

Abstract:
"The dynamic adaptive nature of terrorism requires a systematic and methodical intelligent strategy for terrorism threat assessment and management. Unwitting weaknesses in approach and deficiencies in scope invite strategic surprise. Effective decision-making on managing terrorism risk benefits from insights available from quantitative thinking across the range of significant risk factors. This way of thinking about terrorism is presented in a manner accessible to military and security personnel, emphasizing key conceptual principles and ideas, whilst minimizing technical mathematical detail." [p. 101]

Keywords: Terrorism, Risk modeling, Counter-terrorism.

Purpose:
- The purpose of this paper is to provide an exposition of the basic concepts underlying a structured and objective approach to risk assessment.

Description:
The concepts described include:
- Terrorism threat analysis and scenario development
- Criticality analysis
- Vulnerability analysis
- Capability analysis
- Risk calculation
- Comparison and evaluation of terrorism threats
- Terrorism threat management
- Risk reduction
- Risk avoidance
- Risk shifting
- Acceptance of risk

3.6.7 Threat Levels: The System to Assess the Threat from International Terrorism

Title: Threat Levels: The System to Assess the Threat from International Terrorism
Author(s): National Counter Terrorism Security Office (NaCTSO)
Organization: National Counter Terrorism Security Office (NaCTSO)
Publisher: The Stationery Office
Publishing Location: Norwich, UK
Edition: N/A
Pages: 8
Retrieved from: National Counter Terrorism Security Office website
Hyperlink: http://www.nactso.gov.uk/SiteCollectionDocuments/Threats/Threat-Levels.pdf
Date of Publication: July 2006

Purpose:

- This paper aims to "inform the general public about the process and the national threat level, which applies to the UK as a whole. This document aims to explain what threat levels are and how they are used." [p. 1]

Description:
This document includes the following sections:

- What are threat levels
- How do we decide threat levels
- Who decides threat levels
- Where can I find out what the current national threat level is
- What are response levels and how do they relate to threat levels
- How the public should respond to different national threat levels

3.6.8 Survey of Bioterrorism Risk in Buildings

Title: Survey of Bioterrorism Risk in Buildings
Author(s): Benjamin P. Thompson and Lawrence C. Bank
Organization: N/A
Publisher: American Society of Civil Engineers (ASCE)
Publishing Location: Unavailable
Edition: N/A
Pages: 7-17
Retrieved from: Journal of Architectural Engineering, Vol. 14, No. 1
Hyperlink: N/A
Date of Publication: March 2008

Abstract:
"Due to the lack of data and experience with designing buildings for a bioterrorism hazard, it is important for civil engineering professionals to understand both the way that risk is currently accounted for in the design of a building for a bioterrorism hazard and the methods for analyzing risks to buildings that can be borrowed from risk analysis professionals. This paper provides a literature survey of four subject areas dealing with the risk analysis of bioterrorism applied to buildings: (1) perception of the risk of bioterrorism; (2) risk analysis of bioterrorism; (3) risk management of bioterrorism risks; and (4) risk communication of bioterrorism risks, and includes an example of a simple risk analysis process for a hypothetical building. Bioterrorism presents building design engineers with new challenges. It is a very unpredictable hazard, and very little data exist to guide building designers and decision makers in protecting buildings from this hazard. Designing a building with bioterrorist attacks in mind involves many different disciplines, including, for example, structural, mechanical, and electrical engineering, architecture, landscape architecture, security design professions, and law enforcement. Large consequences are possible in the event of a successful attack, and many building design engineers have little or no experience with defending against a bioterrorist attack. It is important that a reasonable process for analyzing and dealing with these risks be established, and that the process include issues of risk perception and communication within the risk analysis framework." [p. 7]

3.7 Lexicons

3.7.1 Intelligence Experts Group: All-Hazards Risk Assessment Lexicon

Title: Intelligence Experts Group: All-Hazards Risk Assessment Lexicon
Author(s): Simona Verga
Organization: Defence Research and Development Canada (DRDC), Centre for Security Science (CSS)
Publisher: DRDC-CSS
Publishing Location: Unavailable
Edition: Unavailable
Pages: 22
Retrieved from: Note, DRDC-CSS-N-2007-001
Hyperlink: N/A
Date of Publication: 2007

Abstract:
"This document proposes a *lexicon* of key risk terms, to establish a common terminology among partners collaborating on the All-Hazards Risk Assessment project. The definitions included in this lexicon have been compiled by consulting a variety of sources and through iterations with various risk communities. The goal is to have consistent and flexible terms that accommodate as much as possible the specialized terminology in specific risk domains. The hope is that the final document will have wide acceptance, providing a sound basis for the dialog among the project partners, and thus improving the effectiveness of the collaborative effort." [p. i]

3.7.2 Department of Homeland Security Risk Lexicon

Title: Department of Homeland Security Risk Lexicon
Author(s): Department of Homeland Security (DHS) Risk Steering Committee (RSC)
Organization: U.S. Department of Homeland Security
Publisher: U.S. Department of Homeland Security
Publishing Location: United States of America
Edition: 2nd ed.
Pages: 72
Retrieved from: DHS website
Hyperlink: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
Date of Publication: September 2010

Description:

- "The DHS Risk Lexicon makes available a common, unambiguous set of official terms and definitions to ease and improve the communication of risk-related issues for DHS and its partners. It facilitates the clear exchange of structured and unstructured data that is essential to the exchange of ideas and information amongst risk practitioners by fostering consistency and uniformity in the usage of risk-related terminology for the Department." [p. vii]

Additional Information:
This lexicon includes sections on:

- Lexicon process phases
- Definitions
- DHS lexicon governance structure
- Maintenance of the DHS risk lexicon
- Use of the DHS risk lexicon

4 Methodologies, Tools, and Models

Overview

This section contains references which present and discuss methodologies, tools, and models for assessing risk (or a component of risk). It is divided according to the scope of the references, in terms of the hazards or threats that are considered.

- **Section 4.1**: methodologies, tools, and models which take an all-hazard approach to risk assessment.
  Note: Included in this section are references in which the scope of hazards or threats is not explicitly stated, but are general enough to be included under all-hazards.
- **Section 4.2**: methodologies, tools, and models which focus on non-malicious hazards. These references are further divided into sub-groups: Natural hazards (4.2.1), Man-made unintentional hazards (4.2.2), Health hazards (4.2.3), and Multi-hazards (4.2.4).
- **Section 4.3:** methodologies, tools, and models which focus on malicious threats. These references are further divided into sub-groups: Cyber threats (4.3.1), Chemical, Biological, Radiological, Nuclear, and Explosive threats (CBRNE) (4.3.2) and Multi-threats (4.3.3).
- **Section 4.4**: a miscellaneous reference.

4.1 All-Hazards

4.1.1 All Hazards Risk Assessment Methodology Guidelines (2011-2012)

Title: All Hazards Risk Assessment Methodology Guidelines (2011-2012)
Author(s): Public Safety Canada
Organization: Public Safety Canada and Defence Research and Development Canada - Centre for Security Science
Publisher: Unavailable
Publishing Location: Canada
Edition: 1.0 (Initial Version)
Pages: 74
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: December 1st, 2011

Purpose:

- "The purpose of the federal AHRA [All Hazards Risk Assessment] process is to assess and view risks in a standardized fashion using a common set of principles and steps." [p. 1]
- The AHRA process "is meant to create a multi-dimensional, high-level view of risks faced by Canadians, while bringing diverse risks from various sources into the same high-level view." [p. 5]

Scope:

- All-hazards risks
- "Risk assessment specific to the critical infrastructure (CI) sectors is beyond the scope of the federal AHRA methodology." [p. 2]

Audience:

- The AHRA methodology is aimed at federal government institutions in Canada, and supports them in "fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for EM [Emergency Management] planning." [p. 1]

Description:

- "The federal AHRA process is based on a methodology that comprises the following steps, as identified in ISO 31000, "Risk Management - Principles and Guidelines:" [p. 3]
  1. Setting the context
  2. Risk identification
  3. Risk analysis
  4. Risk evaluation
  5. Risk treatment
- This document describes the AHRA methodology, and guides users through its step-by-step process.

4.1.2 Hazard Identification and Risk Assessment Workbook

Title: Hazard Identification and Risk Assessment Workbook
Author(s): Emergency Management Ontario
Organization: Emergency Management Ontario
Publisher: Emergency Management Ontario
Publishing Location: Ontario, Canada
Edition: Unavailable
Pages: 24
Retrieved from: Emergency Management Ontario website
Hyperlink:
http://www.emergencymanagementontario.ca/stellent/groups/public/@mcscs/@www/@emo/documents/abstract/ec159132.pdf
Date of Publication: 2012

Description:

- The Hazard Identification Risk Assessment (HIRA) is a "risk assessment tool that can be used to assess which hazards pose the greatest risk in terms of how likely they are to occur and how great their potential impact may be." [p. 3]

Additional Information:

- The Hazard Identification Risk Assessment process consists of 4 steps:
  - Hazard identification
  - Risk assessment
  - Risk analysis
  - Monitor and review
- For the above steps, this workbook provides worksheets, scoring tables, variables/factors to consider, equations, or examples to assist readers in carrying out the HIRA.

4.1.3 British Columbia Hazard, Risk and Vulnerability Analysis Tool Kit

Title: British Columbia Hazard, Risk and Vulnerability Analysis Tool Kit
Author(s): Ministry of Public Safety and Solicitor General, Provincial Emergency Program
Organization: British Columbia government
Publisher: Unavailable
Publishing Location: British Columbia, Canada
Edition: N/A
Pages: 62
Retrieved from: Emergency Management British Columbia website, formerly the Provincial Emergency Program website
Hyperlink: http://www.pep.bc.ca/hrva/toolkit.html
Date of Publication: January 2004

Purpose:

- "The purpose of the Hazard, Risk and Vulnerability Analysis (HRVA) is:
  to help a community make risk-based choices to address vulnerabilities, mitigate hazards and prepare for response to and recovery from hazard events." [p. i]

Objective:

- "Hazard, Risk and Vulnerability Analysis (HRVA) is not an end in itself. The purpose of hazard, risk and vulnerability analysis planning is to anticipate problems and possible solutions to help save lives and property, reduce damage, and speed a community's recovery.
- The HRVA helps us work towards disaster-resilient communities." [p. i]

Additional Information:

- This document describes each of the steps in the HRVA:
  - Administration
  - Training
  - Gather risk information
  - Hazard and vulnerability identification
  - Risk analysis
  - Risk evaluation
  - Public consultation plan
  - Action plans
- The toolkit also provides forms, sample agendas, checklists, and schedules to assist users through the above steps.

4.1.4 A Proof of Concept Study for Analyzing Hazmat Transportation Risks in an All-Hazards Environment

Title: A Proof of Concept Study for Analyzing Hazmat Transportation Risks in an All-Hazards Environment
Author(s): Samrat Chatterjee and Mark D. Abkowitz
Organization: Department of Civil and Environmental Engineering, Vanderbilt University, TN, USA
Publisher: Taylor & Francis
Publishing Location: Unavailable
Edition: N/A
Pages: 135-151
Retrieved from: Journal of Transportation Safety & Security, Vol. 1, No. 2
Hyperlink: N/A
Date of Publication: June 2009

Abstract:
"Events such as the World Trade Center attacks, Hurricane Katrina, and the Minneapolis bridge collapse have affected society's perception of the risks affecting our lives. It has also led to the realization that a more systematic and holistic approach to risk management is needed, one that takes into consideration natural hazards, manmade accidents, and intentional acts in a single context. This article discusses the early stage development of an all-hazards risk management (AHRM) approach designed to achieve this objective, taking hazardous materials transportation risk into consideration. Utilizing established assessment methods and data sources, relevant risks are expressed in monetary terms, creating a consistent basis from which one can identify those risks that warrant priority attention. An early stage application is presented, one involving an assessment of truck transportation of hazardous materials and earthquakes as two risks threatening several areas within the State of Tennessee, to illustrate the viability of implementing an AHRM approach." [p. 35]

Objective:
- "The immediate challenge in formulating an AHRM approach lies in establishing a common protocol and performance metric to quantify risks posed by various hazards. Preliminary design and testing of a methodology to accomplish this task was the primary objective of this research." [p. 136]

Geographical scope:
- A county

Additional Information:
This paper covers the following sections:
- Literature review of previous efforts to formalize the concept of an all-hazards risk management approach
- Description of the All-Hazards Risk Management (AHRM) approach
- Development of the All-Hazards Risk Management (AHRM) methodology and its application to:
  - Truck transportation of hazardous materials
  - Earthquake
- Conclusions and further research

4.1.5 Oregon Emergency Management (OEM): Hazard Analysis Methodology

Title: Oregon Emergency Management (OEM): Hazard Analysis Methodology
Author(s): Oregon Emergency Management
Organization: Oregon Emergency Management
Publisher: Oregon Emergency Management
Publishing Location: Oregon, United States of America
Edition: Unavailable
Pages: 8
Retrieved from: Oregon State government website
Hyperlink:
http://www.oregon.gov/OMD/OEM/docs/library/oem_hazard_analysis_methodology_5_08.pdf?ga=t
Date of Publication: Unavailable, but updated May 2008

Description:

- This document describes a hazard analysis methodology which was first developed by FEMA in 1983. Over the years, it has been refined by Oregon Emergency Management (OEM).
- This methodology was used by Oregon's 36 counties. In addition, several cities have also conducted hazard analysis using this method.
- Vulnerability and probability are two key components of the methodology. The method "provides the jurisdiction with a sense of hazard priorities, or relative risk. It doesn't predict the occurrence of a particular hazard, but it does "quantify" the risk of one hazard compared with another. By doing this analysis, planning can first be focused where risk is greatest." [p. 1]
- This methodology is a "big picture tool", and should only be considered as one tool amongst others.
- This document also includes a hazard analysis matrix worksheet, a scoring guide, and several examples.

4.1.6 Handbook for Conducting a GIS-Based Hazards Assessment at the County Level

Title: Handbook for Conducting a GIS-Based Hazards Assessment at the County Level
Author(s): Susan L. Cutter, Jerry T. Mitchell, and Michael S. Scott
Organization: Hazards Research Lab, Department of Geography, University of South Carolina
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 55
Retrieved from: Federal Emergency Management Agency (FEMA) website
Hyperlink: http://www.training.fema.gov/emiweb/edu/docs/hrm/Session%206%20-%20Handbook%20GIS-Based%20Hazards%20Assessment.pdf
Date of Publication: November 1997

Description:

- This handbook describes a hazards assessment methodology using an all-hazards approach.
- It has been created to "provide county emergency managers with a method for identifying those areas most vulnerable to hazards within their counties. Throughout the document, the text is accompanied by numerous tables, figures, and flow diagrams to facilitate a successful completion of a hazards assessment for your county." [p. 1]
- "The end product of this assessment is a detailed series of data that integrates the social vulnerability of the population with the geographic distribution of potential hazards. These data can be mapped to increase your understanding of where the most vulnerable areas of your county are located." [p .2]
- This assessment is a valuable instrument for pre-impact planning, post event response, and mitigation.

Additional Information:
**Note*: This handbook was prepared for the South Carolina Emergency Preparedness Division, Office of the Adjutant General.

4.1.7 Threat and Hazard Identification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201

Title: Threat and Hazard Identification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201
Author(s): United States Department of Homeland Security (DHS)
Organization: United States Department of Homeland Security (DHS)
Publisher: United States Department of Homeland Security (DHS)
Publishing Location: Unavailable
Edition: 1st ed.
Pages: 22
Retrieved from: DHS Comprehensive Preparedness Guide (CPG) 201, from FEMA's Resource Library website
Hyperlink: http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5823
Date of Publication: April 2012

Description:

- "This Threat and Hazard Identification and Risk Assessment (THIRA) guide provides a comprehensive approach for identifying and assessing risks and associated impacts. It expands on existing local, tribal, territorial, and state Hazard Identification and Risk Assessments (HIRAs) and other risk methodologies by broadening the factors considered in the process, incorporating the whole community throughout the entire process, and by accounting for important community-specific factors." [p. 1]

Additional Information:
"The THIRA guide describes a step-by-step process:

- Step One assesses the various threats and hazards facing a community of any size.
- Step Two assesses the vulnerability of the community to those hazards using varying time, season, location, and community factors.
- Steps Three and Four estimate the consequences of those threats and hazards impacting the community and, through the lens of core capabilities, establish capability targets.
- Step Five captures the results of the THIRA process to set an informed foundation for planning and preparedness activities across prevention, protection, mitigation, response, and recovery." [p. 1]

4.1.8 Threat and Hazard Identification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201, Supplement 1: Toolkit

Title: Threat and Hazard Identification and Risk Assessment Guide, Comprehensive Preparedness Guide (CPG) 201, Supplement 1: Toolkit
Author(s): United States Department of Homeland Security (DHS)
Organization: United States Department of Homeland Security (DHS)
Publisher: United States Department of Homeland Security (DHS)
Publishing Location: United States of America
Edition: 1st ed.
Pages: 26
Retrieved from: DHS Comprehensive Preparedness Guide (CPG) 201, from FEMA's Resource Library website
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=5825
Date of Publication: April 2012

Description:
"This toolkit provides resources and information, data sources, and templates to support the conduct of a Threat and Hazard Identification and Risk Assessment (THIRA) as described in the first edition of the Comprehensive Preparedness Guide 201: Threat and Hazard Identification and Risk Assessment Guide." [p. 1]

4.1.9 Threat and Hazard Identification and Risk Assessment Process: Worksheet Templates

Title: Threat and Hazard Identification and Risk Assessment Process: Worksheet Templates
Author(s): U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
Organization: U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
Publisher: U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: Unavailable
Pages: 20
Retrieved from: FEMA's Resource Library website
Hyperlink: http://www.fema.gov/library/viewRecord.do?fromSearch=fromsearch&id=5956
Date of Publication: May 2012

Description:
"This document includes sample worksheets for the Threat and Hazard Identification and Risk Assessment as described in Comprehensive Preparedness Guide (CPG) 201. These worksheets should be used only as examples and not considered prescriptive or inclusive of all possible approaches." [p. 1]

4.1.10 Community Resilience System Initiative (CRSI) Steering Committee Final Report - A Roadmap to Increased Community Resilience

Title: Community Resilience System Initiative (CRSI) Steering Committee Final Report - A Roadmap to Increased Community Resilience
Author(s): Community and Regional Resilience Institute
Organization: Community and Regional Resilience Institute
Publisher: Unavailable
Publishing Location: United States of America
Edition: Unavailable
Pages: 156
Retrieved from: N/A
Hyperlink: http://www.resilientus.org/library/CRSI_Final_Report-1_1314792521.pdf
Date of Publication: August 2011

Description:

- "This report presents the findings of the Community Resilience System Initiative (CRSI) Steering Committee…
- The CRSI was a 15-month collaborative process charged with determining what American communities need in order to become more resilient to the variety of threats they face (natural disasters, economic threats and recessions, and human-induced events such as oil spills and acts of terrorism) and recommending a concrete course of action that will support communities in their resilience-building efforts….
- The CRSI involved more than 150 practitioners and researchers from diverse sectors and disciplines who worked in groups to help inform the development of the Community Resilience System (CRS), a practical, web-enabled process that helps communities to assess, measure, and improve their resilience to threats and disruptions of all kinds, and ultimately be rewarded for their efforts. [p. vii-viii]

Additional Information:
This report is broken down into the following sections:

- Introduction
- "Community Resilience Overview – This section includes definitions and outlines the analytical framework that CRSI participants and CARRI co-developed to help communities assess their resilience. It also describes the benefits communities receive from improving their resilience.
- Description of the CRS – This section explains how the web-enabled Community Resilience System works and provides details (supporting resources, benefits, outcomes, etc.) for each of the six stages in the resilience-building process.
- Observations and Next Steps for Increasing Community Resilience – This section includes observations from the CRSI Steering Committee on what national and regional associations and organizations, state and local governments, and the federal government should do to support community resilience-building efforts in general and dissemination and use of the CRS in particular. It also describes activities that the Steering Committee would like to see CARRI, the CRSI, and its partners accomplish including additional convening around the issue of securing resilience benefits for communities and efforts to foster and grow a strengthened national culture of resilience." [p. 2]

4.1.11 Guide to Risk Assessment Tools, Techniques and Data

Title: Guide to Risk Assessment Tools, Techniques and Data
Author(s): Department for Communities and Local Government
Organization: Department for Communities and Local Government
Publisher: Communities and Local Government Publications
Publishing Location: Wetherby, UK
Edition: Unavailable
Pages: 76
Retrieved from: Fire Research Series 5/2009, Communities and Local Government website
Hyperlink: http://www.communities.gov.uk/documents/fire/pdf/guideriskassessmenttoolsFRS5.pdf
Date of Publication: September 2009

Objective:

- "This guide aims to support the conduct of risk assessments by LRFs [Local Resilience Forums] in the context of civil contingency planning and by FRS [Fire and Rescue Service] in the context of IRMP [Integrated Risk Management Plan]. It provides:
    - an overview of the form of risk assessment that is possible for each risk category
    - identifies specific tools, techniques and data where they exist and summarises these
    - notes the limitations of current tools, techniques and data
    - provides references and sources for use by LRFs and FRSs." [p. 10]

Scope:

- "This guide is limited to the use of risk assessment in the context of LRFs and FRS IRMPs…The focus is on tools and data that support civil contingency risk assessment and related planning." [p. 10]

Description:

- This document provides information on tools, techniques and data for risk assessment.

Additional Information:

- This document is structured by risk categories. They are:
    - Transport
    - Fire and Explosion
    - Weather
    - Pollution
    - Industrial Infrastructure
    - Human and Animal Health
    - Structural Collapse
    - Terrorist and Protest
- These risk categories are broken down further into more specific sub-sections. For each sub-section, the following information is provided:
    - Overview
    - Tools and techniques
    - Data sources
- This document also discusses domino effects of individual risks, and provides generic tools to address them.

4.1.12 National Emergency Risk Assessment Guidelines (NERAG)

Title: National Emergency Risk Assessment Guidelines (NERAG)
Author(s): Tasmanian State Emergency Service, on behalf of the Risk Assessment Measurement and Mitigation Sub-Committee
Organization: National Emergency Management Committee
Publisher: Tasmanian State Emergency Service
Publishing Location: Hobart, TAS, AU
Edition: Unavailable
Pages: 57
Retrieved from: Emergency Management Australia website
Hyperlink:
http://www.em.gov.au/Documents/National%20Emergency%20Risk%20Assessment%20Guidelines%20October%202010.PDF
Date of Publication: October 2010

Purpose:

- "This document has been prepared to improve the consistency and rigour of emergency risk assessments, increase the quality and comparability of information on risk and improve the national evidence-base on emergency risks in Australia.
- The NERAG provide a contextualised emergency risk assessment methodology consistent with the Australian/New Zealand Standard *AS/NZS ISO31000:2009 Risk management – Principles and guidelines*." [p. 4]

Scope:

- The method is scalable, and can be used at local, regional, state/territory and national levels.
- It considers all-hazards.
- The guidelines focus on risk assessment, but also provides guidance for establishing the context, treating risks, as well as communication and consultation.

Description:
The guidelines provide:

- "Information on and a methodology for risk assessments, including their preparation, conduct, and outputs for emergency events...
- "Explicit risk criteria and reporting templates." [p. 6]

Note: There is a CD which supplements this guideline by providing templates and tools.

4.1.13 Victoria's State-Level Emergency Risk Assessment Method

Title: Victoria's State-Level Emergency Risk Assessment Method
Author(s): Paul Gabriel
Organization: Emergency Management Australia
Publisher: Unavailable
Publishing Location: Australia
Edition: N/A
Pages: 5-10
Retrieved from: Australian Journal of Emergency Management, Vol. 24, No. 1
Hyperlink:
http://www.em.gov.au/Documents/Victoria%20s%20state%20level%20emergency%20risk%20assessment%20method.PDF
Date of Publication: February 2009

Abstract:
"Victoria's State Emergency Mitigation Committee has developed a method for initial comparative assessment of emergency-related risks at state level. Adapting existing municipal-level models, a method has been developed and successfully implemented. The main adaptations have been the use of a curve to represent the risk rating, the placement of coloured risk zones on the graph, the recalibration of consequence descriptors to the state-level context, and the use of logarithmic scales." [p. 5]

Audience:
- This risk assessment method is aimed at state governments, and is intended to support their decisions regarding investment in mitigation.

Description:
- The risk assessment method considers the entire state as one entity. Hence, the assessment provides a high-level view of major risks.

4.1.14 Community Emergency Risk Assessment (CERA)

Title: Community Emergency Risk Assessment (CERA)
Author(s): Victorian State Emergency Service (VICSES)
Organization: Victorian State Emergency Service (VICSES)
Publisher: Unavailable
Publishing Location: Victoria, Australia
Edition: 2011 Trial
Pages: 45
Retrieved from: Victoria State Emergency Service website
Hyperlink: http://www.ses.vic.gov.au/prepare/em-planning/em-partners-resources/community-emergency-risk-assessment-manual
Date of Publication: October 2011

Description:

- The Community Emergency Risk Management (CERM) process has been updated from the 1998 version to align to the guidelines and methodologies of *ISO 31000*, *National Emergency Risk Assessment Guidelines (NERAG)* and S*tate Emergency Risk Assessment Methodology (SERAM)*, and to incorporate valuable outputs of significant natural disasters over the past decade.
- "The Community Emergency Risk Assessment (CERA) process provides a simple, efficient yet powerful approach for communities, municipalities and their respective Municipal Emergency Planning Committees (MEMPCs) across Victoria to identify and assess emergency risks and to help inform and drive responsive actions." [p. 3]
- "The CERA process...is explicitly designed to align with *ISO 31000:2009* – a global standard for risk management. It reflects a 5-step, iterative process that is supported by two supporting pillars, namely:
    - Communicate and Consult
    - Monitor and Review
- This manual provides a detailed description for each step and supporting pillars. In addition, the CERA process is supported by additional tools, in particular, an Excel-based workbook wherein risk identification and analysis can be performed and documented quickly and consistently across the full breadth of municipalities that comprise the state of Victoria." [p. 5]

Note: The CERA Tool is available upon request from your local SES Regional Office (Australian).

4.1.15 National Risk Assessment in the Netherlands: A Multi-Criteria Decision Analysis Approach

Title: National Risk Assessment in The Netherlands: A Multi-Criteria Decision Analysis Approach
Author(s): Erik Pruyt and Diederik Wijnmalen
Organization: N/A
Publisher: Springer
Publishing Location: Berlin & Heildelberg, Germany
Edition: N/A
Pages: 133-143
Retrieved from: Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems, Lecture notes in Economic Systems and Mathematical Systems, vol. 634, part 2
Hyperlink: http://www.springerlink.com/content/l60t423960560140/, but available for free on google books
Date of Publication: 2010

Abstract:
"Nowadays, National Safety and Security issues receive much attention in many countries. In 2007, the Dutch government approved a National Safety and Security Strategy based on a multi-criteria analysis approach to classify potential threats and hazards. The general methodology of this Dutch National Risk Assessment and the specific multi-criteria-based approach developed for it are presented in this paper. Five issues are discussed here: the objectives, requirements and criteria of the risk assessment; the multi-criteria methods used; the pluralistic weighting approach; the sensitivity and robustness analyses; and the outcomes of the Dutch National Risk Assessment." [p. 133]

Key words: National Risk Assessment (NRA), National safety and security strategy, Multi-criteria decision analysis (MCDA)

Objective:

- "The objective of the NRA [National Risk Assessment] is to develop a robust classification of incident scenarios in terms of impact and likelihood in order to help the Dutch government decide about what additional capabilities to organise for dealing with plausible and potentially devastating threats and hazards. That requires a comparison and classification of a multitude of different threats and hazards at the national level." [p. 135]

4.1.16 Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands

Title: Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands
Author(s): Working Group of: Dr. Hans Bergmans, Ir. Jasper van der Horst, Dr. Leon Janssen, Dr. Erik Pruyt, Dr. Vic Veldheer, Drs. Diederik Wijnmalen, General Intelligence and Security Service, Ir. Mark Bökkerink, Drs. Pamela van Erve, Drs. Juliette van de Leur
Organization: N/A
Publisher: Unavailable
Publishing Location: Netherlands
Edition: Unavailable
Pages: 102
Retrieved from: Mitigating Spatial Relevant Risks in European Regions and Towns (MiSRaR) website
Hyperlink:
http://www.misrar.nl/UserFiles/File/BP_1_ZHZ_annex%202%20National_Riskassesment__English(1).pdf
Date of Publication: October 2009

Purpose:
"The purpose of the guide is:

- To describe the method used for scenario development, national risk assessment and capability analysis;
- To establish and justify the choices made;
- To provide a guide for people who have to work with the national safety and security strategy;

This guide makes clear to people who have to work with the national safety and security strategy how this method works. It should also serve as a foundation for those drawing up incident scenarios and for those carrying out the national risk assessment and capability analysis in 2009 and later." [p. 7]

Description:

- This guide presents a method for creating scenarios, scoring impact and likelihood, and conducting capability analysis.
- The guide also provides background information to support the choices made throughout the process.
- This method is "an aid that gives policy makers a framework - in addition to other frameworks - to weigh up the threats, and be able to make policy choices more effectively." [p. 12]

Additional Information:

- The National Safety and Security Method has three phases:
  1. Scenario development
  2. National risk assessment
  3. Capability analysis
- For the phases listed above, this document provides practical guidance through examples, checklists, tables, constraints, and requirements.

4.1.17 Regional Risk Assessment in the Netherlands

Title: Regional Risk Assessment in the Netherlands
Author(s): Unavailable, introduction by Ruud Houdijk
Organization: Mitigating Spatial Relevant Risks in European Regions and Towns (MiSRaR)
Publisher: Mitigating Spatial Relevant Risks in European Regions and Towns (MiSRaR)
Publishing Location: The Hague, the Netherlands
Edition: Unavailable
Pages: 14
Retrieved from: 1st MiSRaR seminar, 27th May 2010
Hyperlink:
http://www.misrar.nl/UserFiles/File/BP_1_ZHZ_annex%201%20Regional%20risk%20assessment%20in%20The%20Netherlands.pdf
Date of Publication: May 2010

Description:
"From 2011 onwards, in The Netherlands the 25 so-called Safety Regions…are by law required to develop a regional risk assessment, also referred to as 'regional risk profile'. To assist the regions in this endeavor and realize a common practice and understanding, in 2009 a 'National Guideline on Regional Risk Assessment' has been developed, as a joint initiative of the Dutch Association for Fire fighting and Disaster management, the Dutch Association for Medical Emergency Management, the Council of Chief Constables and the Council of Municipal Disaster Management, in close cooperation with the Ministry of the Interior and Kingdom Relations and experts from nearly all Dutch Safety Regions. In this guideline is described how the regions can identify hazards, analyze them, and support the process of political decision making on risk management policies. 24 of the 25 regions have decided to implement this guideline, enabling a comparison between the regional risk assessments. Moreover, to ensure a close connection between the regional assessments and the national risk assessments, the method as described in the national guideline is based upon the method used by the Dutch central government. This method is scientifically sound, and consists of a combination of tried and tested sub-methods on the one hand, and new elements on the other, developed to meet the requirements (including uniformity and comparability) of national and regional risk assessment in The Netherlands." [p. 3]

Additional information:
"This paper gives an outline of the 'Dutch approach to risk assessment'.

- Firstly in chapter 2 the organization of the Dutch government is described, for a better understanding of the Dutch approach.
- This is followed by a description of the underlying reasons to implement a regional risk assessment in chapter 3.
- In chapter 4 the interpretation of the concept of risk is presented, followed by a description of the process for risk assessment and policy making in chapter 5.
- In chapters 6 to 8 the distinct steps of the risk assessment are presented, namely hazard identification, risk analysis and risk evaluation.
- Chapter 9 then concentrates on the translation from the risk assessment into concrete risk management policies.
- Concluding this essay, in the epilogue a vista is given upon the usability of the Dutch approach for the MiSRaR project." [p. 3]

4.1.18 Ranking the Risks from Multiple Hazards in a Small Community

Title: Ranking the Risks from Multiple Hazards in a Small Community
Author(s): Hua Li, George E. Apostolakis, Joseph Gifun, William VanSchallkwyk, Susan Leite, and David Barber
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 438-456
Retrieved from: Risk Analysis, Vol. 29, No. 3
Hyperlink: N/A
Date of Publication: March 2009

Abstract:
"Natural hazards, human-induced accidents, and malicious acts have caused great losses and disruptions to society. After September 11, 2001, critical infrastructure protection has become a national focus in the United States and is likely to remain one for the foreseeable future. Damage to the infrastructures and assets could be mitigated through pre-disaster planning and actions.
A systematic methodology was developed to assess and rank the risks from these multiple hazards in a community of 20,000 people. It is an interdisciplinary study that includes probabilistic risk assessment (PRA), decision analysis, and expert judgment. Scenarios are constructed to show how the initiating events evolve into undesirable consequences. A value tree, based on multi-attribute utility theory (MAUT), is used to capture the decisionmaker's preferences about the impacts on the infrastructures and other assets. The risks from random failures are ranked according to their expected performance index (PI), which is the product of frequency, probabilities, and consequences of a scenario. Risks from malicious acts are ranked according to their PI as the frequency of attack is not available. A deliberative process is used to capture the factors that could not be addressed in the analysis and to scrutinize the results. This methodology provides a framework for the development of a risk-informed decision strategy. Although this study uses the Massachusetts Institute of Technology campus as a case study of a real project, it is a general methodology that could be used by other similar communities and municipalities." [p. 438]

Key words: Infrastructures, natural hazards, risk ranking, terrorism

4.1.19 Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework

Title: Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework
Author(s): Bilal M. Ayyub, William L. McGill, and Mark Kaminskiy
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 789-801
Retrieved from: Risk Analysis, Vol. 27, No. 4
Hyperlink: N/A
Date of Publication: August 2007

Abstract:
"This article develops a quantitative all-hazards framework for critical asset and portfolio risk analysis (CAPRA) that considers both natural and human-caused hazards. Following a discussion on the nature of security threats, the need for actionable risk assessments, and the distinction between asset and portfolio-level analysis, a general formula for all-hazards risk analysis is obtained that resembles the traditional model based on the notional product of consequence, vulnerability, and threat, though with clear meanings assigned to each parameter. Furthermore, a simple portfolio consequence model is presented that yields first-order estimates of interdependency effects following a successful attack on an asset. Moreover, depending on the needs of the decisions being made and available analytical resources, values for the parameters in this model can be obtained at a high level or through detailed systems analysis. Several illustrative examples of the CAPRA methodology are provided." [p. 789]

Key words: All hazards; consequence; critical asset protection; decision; homeland security; risk analysis; security; terrorism; threat; vulnerability

4.1.20 Hazards Risk Assessment Methodology for Emergency Managers: A Standardized Framework for Application

Title: Hazards Risk Assessment Methodology for Emergency Managers: A Standardized Framework for Application
Author(s): Norman Ferrier and C. Emdad Haque
Organization: N/A
Publisher: Kluwer Academic Publishers
Publishing Location: Netherlands
Edition: N/A
Pages: 271-290
Retrieved from: Natural Hazards, Vol. 28, No. 2-3
Hyperlink: N/A
Date of Publication: March 2003

Abstract:
"The public and the decision and policy makers who serve them too often have a view of community risks that is influenced and distorted significantly by media exposure and common misconceptions. The regulators and managers, responsible for planning and coordination of a community's mitigation, preparedness, response and recovery efforts, are originated from a variety of disciplines and levels of education. Not only must these individuals deal with the misconceptions of their communities, but also frequently lack a basic methodology for the assessment of risks. The effective planning of mitigation and response are, however, directly dependent upon the understanding of the complexities, types, and nature of risks faced by the community, determining the susceptible areas, and conceptualizing human vulnerability.

In this study, a review of the existing literature on both the conceptual underpinnings of risk and its assessment is attempted. A standardized framework is proposed for use by all emergency managers, regardless of training or education. This framework consists of the numerical ranking of the frequency of the event in the community, multiplied by a numerical ranking of the severity or magnitude of an event in a given community, based upon the potential impact characteristics of a `worst-case' scenario. This figure is then multiplied by a numerical ranking indicating the Social Consequence; a combination of community perception of risk level and collective will to address the problem. The resulting score, which is not strictly scientific, would permit emergency managers from a variety of backgrounds to compare levels of community exposure to such disparate events as hazardous materials spills and tornadoes, and to set priorities for both mitigation efforts and for the acquisition of response needs, within the availability of community resources." [p. 271]

Description:
"This study begins by addressing some definitional and conceptual ambiguities. It examines the nature of risk and its components, as well as the identification of hazards faced by the community in real-life. The importance of assessment of vulnerability is also critically reviewed. While the local level data and scientific methods for risk assessment are scanty, this research proposes the use of a standardized methodology to permit emergency managers and others to evaluate various types of dissimilar risks, as well as the potential for impact by those risks on the community. Finally, the advantages and disadvantages of such a system are explored." [p. 272]

4.2 Non-Malicious Hazards

4.2.1 Natural Hazards

4.2.1.1 Understanding Your Risks: Identifying Hazards and Estimating Losses

Title: Understanding Your Risks: Identifying Hazards and Estimating Losses
Author(s): Federal Emergency Management Agency (FEMA)
Organization: Federal Emergency Management Agency (FEMA)
Publisher: Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: Version 1.0
Pages: 168
Retrieved from: Mitigation Planning How-To Guide #2: (FEMA 386-2)
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=1880
Date of Publication: August 2001

Description:
"Mitigation Planning How-To Guide # 2 (FEMA 386-2), the second guide in the State and Local Mitigation Planning How-To Series, provides step-by-step guidance on how to perform a risk assessment. Through a series of general and hazard-specific guidance and worksheets, the guide will help State, Indian Tribal, and local planning teams determine (1) which natural hazards could affect a jurisdiction; (2) what areas of the jurisdiction are vulnerable to the hazards; (3) what assets will be affected; and (4) to what degree they will be affected, as measured through dollar losses. This Guide is multi-hazard in scope, addressing flood, earthquake, tsunami, tornado, coastal storm, landslide and wildfire hazards. For communities dealing with multiple hazards, guidance is also provided on how to develop a composite loss estimate. Once the risk assessment is completed, State, Indian Tribal, and local officials will have the information necessary to develop a strategy and plan for reducing their losses.[16]"

Additional Information:

- This guide is specific to the second phase of the Natural Hazard Mitigation Process, "Assess Risks". It addresses each of the 4 phases of assessing risks:
  - Identify hazards
  - Profile hazard events
  - Inventory assets
  - Estimate losses
- This how-to-guide does not require complicated statistical analysis. Rather, it is intended to help a community or state develop a basic estimate of the potential losses that may be incurred from one event.

[16] From http://www.fema.gov/library/viewRecord.do?id=1880

4.2.1.2 HAZUS-MH: FEMA's Methodology for Estimating Potential Losses from Disasters

Title: HAZUS-MH: FEMA's Methodology for Estimating Potential Losses from Disasters
Author(s): Federal Emergency Management Agency (FEMA)
Organization: Federal Emergency Management Agency (FEMA)
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: N/A
Retrieved from: Federal Emergency Management Agency (FEMA) website
Hyperlink: http://www.fema.gov/plan/prevent/hazus/
Date of Publication: Unavailable

This website provides an overview of HAZUS-MH, as well as information on how to acquire the software.

Description:
"Hazus is a nationally applicable standardized methodology that contains models for estimating potential losses from earthquakes, floods, and hurricanes. Hazus uses Geographic Information Systems (GIS) technology to estimate physical, economic, and social impacts of disasters. It graphically illustrates the limits of identified high-risk locations due to earthquake, hurricane, and floods. Users can then visualize the spatial relationships between populations and other more permanently fixed geographic assets or resources for the specific hazard being modeled, a crucial function in the pre-disaster planning process. Hazus is used for mitigation and recovery as well as preparedness and response. Government planners, GIS specialists, and emergency managers use Hazus to determine losses and the most beneficial mitigation approaches to take to minimize them. Hazus can be used in the assessment step in the mitigation planning process, which is the foundation for a community's long-term strategy to reduce disaster losses and break the cycle of disaster damage, reconstruction, and repeated damage. Being ready will aid in recovery after a natural disaster…

Additional Information:
Ordering Hazus-MH:
Federal, State and local government agencies and the private sector can order the latest version of Hazus free-of-charge on-line by visiting the FEMA Map Service Center (MSC) Web Store at msc.fema.gov. For more information about how to set up your account with the MSC and place your order, please refer to the Hazus-MH Overview flyer.[17]"

[17] From http://www.fema.gov/plan/prevent/hazus

4.2.1.3 Using HAZUS-MH for Risk Assessment (How-To Guide)

Title: Using HAZUS-MH for Risk Assessment (How-To Guide)
Author(s): Federal Emergency Management Agency (FEMA)
Organization: Federal Emergency Management Agency (FEMA)
Publisher: Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: Unavailable
Pages: 226
Retrieved from: FEMA 433, HAZUS-MH Risk Assessment and User Group Series, from the Federal Emergency Management Agency (FEMA) Resource Library website
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=1985
Date of Publication: August 2004

Description:

- This How-To-Guide is designed to help prepare standardized, scientifically-based risk assessments using the Hazards U.S. Multi-Hazard (HAZUS-MH) software. The Federal Emergency Management Agency (FEMA) prepared this guide based on field-implemented HAZUS-MH risk assessment pilot projects across the country that are responding to the requirements of the Disaster Mitigation Act of 2000 (DMA 2000). FEMA prepared this guide for users who have had exposure to HAZUS-MH and are interested in using HAZUS-MH to support risk assessment studies." [p. vii]

Additional Information:

- "The sections of this guide are organized around the five steps of conducting a risk assessment using HAZUS-MH. Each step includes:
  - Text and graphics that describe the risk assessment steps
  - Instructions and corresponding HAZUS-MH screen captures to support the steps
  - Practical implementation examples and lessons learned from field-based pilot projects
  - Worksheets and associated job aids as training tools to help you complete each step" [p. xi]
- The five steps for using HAZUS-MH to complete a risk assessment are:
  1. Identify Hazards
  2. Profile Hazards
  3. Inventory Assets
  4. Estimate Losses
  5. Consider Mitigation Options

4.2.1.4 Assessing Risk

Title: Assessing Risk
Author(s): Tony Pearce (Ed.)
Articles by:
Trevor Jones,
Alan Sharp,
Craig Arthur, Anthony Schofield and Bob Cechet,
National Flood Risk Advisory Group,
Russell Stevens, Gordon Hall, Dr. Jane Sexton,
Karl Sullivan of the Insurance Council of Australia,
Ryan Crompton and John McAneney,
Dr. Kevin Tolhurst, Brett Shields, Derek Chong
Organization: Emergency Management Australia and Geoscience Australia
Publisher: Grey Worldwide Canberra
Publishing Location: Australia
Edition: Special Edition #1
Pages: 60
Retrieved from: Australian Journal of Emergency Management, vol. 23, no. 4
Hyperlink: http://www.em.gov.au/Documents/AJEM%20-%20Volume%2023%20-%20Issue%20No%204%20-%20Nov08.PDF
Date of Publication: November 2008

Description:

- "This Special Issue has the theme 'Assessing Risk' and its papers address current progress and future directions of risk assessment for the draft set of priority natural hazards in the National Risk Assessment Framework.
- The papers collectively give a national overview of current all hazards risk assessment including the methods, data requirements, and issues from a government and insurance industry point of view." [p. 6]

Additional Information:
The papers included in this Special Issue are:

1. Advances in Risk Assessment for Australian Emergency Management
2. Assessing Risk from Meteorological Phenomena Using Limited and Biased Databases
3. Assessing the Impacts of Tropical Cyclones
4. Flood Risk Management in Australia
5. Tsunami Planning and Preparation in Western Australia: Application of Scientific Modelling and Community Engagement
6. Policy Implications of Future Increases in Extreme Weather Events Due to Climate Change
7. The Cost of Natural Disasters in Australia: The Case for Disaster Risk Reduction
8. Phoenix: Development and Application of a Bushfire Risk Management Tool

4.2.1.5 Risk Assessment in Risk Management Programs

Title: Risk Assessment in Risk Management Programs
Author(s): Tony Pearce (Ed.)
Articles by:
Paul Gabriel,
Meryl Sherrah,
Gerry Byrne,
Brian Hine, Mark Stephens and Bob Flett,
Wendy Saunders, Phil Glassey,
Andrew Leventhal and Geoff Withycombe,
Monica Osuchowski,
Nick Nicolopoulos and Emily Hansen
Organization: Emergency Management Australia and Geoscience Australia
Publisher: Grey Worldwide Canberra
Publishing Location: Australia
Edition: Special Edition #2
Pages: 79
Retrieved from: The Australian Journal of Emergency Management, Vol. 24, No. 1
Hyperlink: http://www.em.gov.au/Documents/AJEM%20Volume%2024%20%20No%201%20-%20COMPLETE.PDF
Date of Publication: February 2009

Description:

- "The November 2008 special edition of AJEM gave many examples of methods that are used to produce risk assessment tools and information. This second special edition presents state of the art applications of these approaches by emergency managers, planners and technical specialists in risk management projects to achieve long-term risk reduction." [p. 2]

Additional Information:
The papers included in this Special Edition are:

1. Victoria's state-level emergency risk assessment method
2. A Fresh Approach to Development Assessment in Bushfire Protection Areas
3. I-Zone Planning: Supporting Frontline Firefighters
4. The Wildfire Project: An Integrated Spatial Application to Protect Victoria's Assets from Wildfire
5. Taking a risk-based approach for landslide planning: An outline of the New Zealand landslide
6. Landslide Risk management for Australia
7. Bringing Information management Practices to Natural Disaster Risk Reduction
8. How well prepared are Australian Communities for Natural Disasters and Fire Emergencies?

4.2.1.6 Assessing Physical Vulnerability for Multi-Hazards Using an Indicator-Based Methodology

Title: Assessing Physical Vulnerability for Multi-Hazards Using an Indicator-Based Methodology
Author(s): M.S. Kappes, M. Papathoma-Köhle, M. Keiler
Organization: University of Vienna, Geomorphic Systems and Risk Research Unit
Publisher: Elsevier Ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 577-590
Retrieved from: Applied Geography, vol. 32, no. 2
Hyperlink: N/A
Date of Publication: March 2012

Abstract
"Globally, many built-up areas are threatened by multiple hazards which pose significant threat to humans, buildings and infrastructure. However, the analysis of the physical vulnerability towards multiple hazards is a field that still receives little attention although vulnerability analysis and assessment can contribute significantly to risk reduction efforts. Indicator-based vulnerability approaches are flexible and can be adjusted to the different hazards as well as to specific user needs. In this paper, an indicator-based vulnerability approach, the PTVA (Papathoma Tsunami Vulnerability Assessment), was further developed to be applicable in a multi-hazard context. The resulting multi-hazard version of the PTVA consists of four steps: the identification of the study area and relevant hazards as well as the acquisition of hazard information, the determination of vulnerability indicators and collection of data, the weighting of factors and vulnerability assessment and finally, the consideration of hazard interactions.
After the introduction of the newly developed methodology a pilot application is carried out in the Faucon municipality located in the Barcelonnette basin, Southern French Alps. In this case study the vulnerability of buildings to debris flows, shallow landslides and river flooding for emergency planning and for general risk reduction purposes is assessed. The implementation of the methodology leads to reasonable results indicating the vulnerable buildings and supporting the priority setting of different end-users according to their objectives. The constraints of the presented methodology are: a) the fact that the method is not hazard-intensity specific, thus, vulnerability is measured in a rather qualitative and relative way and b) the high amount of data required for its performance. However, the advantage is that it is a flexible method which can be applied for the vulnerability analysis in a multi-hazard context but also it can be adjusted to the user-specific needs to support decision-making." [p. 577]

Keywords: Physical Vulnerability; Vulnerability indicators; Multi-hazard; Decision-making

Highlights:

- Indicator-based approach to assess physical vulnerability of elements at risk.
- Vulnerability assessment methodology designed for multi-hazard.
- Promising and flexible method to support decision-making for different users and objectives.

4.2.1.7 Loss of Life Estimation in Flood Risk Assessment: Theory and Application

Title: Loss of Life Estimation in Flood Risk Assessment: Theory and Application
Author(s): Sebastiaan Nicolaas Jonkman
Organization: Delft University
Publisher: Delft Hydraulics
Publishing Location: Unavailable
Edition: N/A
Pages: 354
Retrieved from: PhD Thesis, Evaluation, Delft University
Hyperlink: http://safecoast.org/editor/databank/File/SNJonkman_dissertation_smallest.pdf
Date of Publication: 2007

Description:
"Quantitative risk analysis is generally used to quantify the risks associated with accidents in a technical system. The resulting risk estimates, expressing the combination of probabilities and consequences of a set of possible accidents, provide the input for risk evaluation and decision-making. One of the most important types of consequences of accidents concerns the loss of human life. In general, there is limited insight in the magnitude of loss of life caused by accidents, and no general methodology that can be used to estimate loss of life for different event types is available. In particular in the field of flood risk assessment, limited insight exists in the number of fatalities that can result from the flooding of low-lying areas protected by flood defences**.** In the first part of this thesis a general approach for loss of life estimation and risk quantification is proposed. The second part focuses on the estimation of loss of life caused by floods." [p. 1]

Additional Information:
This paper is divided into the following sections:

- Part one: A General Approach for Loss of Life Estimation and Risk Quantification:
  - General approach for loss of life estimation
  - General approach for the quantification of individual and societal risk
  - Uncertainties in loss of life estimates
- Part two: Loss of Life estimation and flood risk assessment
  - Loss of life in floods: Overview and analysis of available information
  - Review of models for the estimation of loss of human life caused by floods
  - A method for the estimation of loss of life caused by floods
- Case studies:
  - Preliminary analysis of loss of life caused by the flooding of New Orleans after hurricane Katrina
  - Flood risk assessment for dike ring South Holland

4.2.1.8 Quantifying Social Vulnerability: A Methodology for Identifying Those at Risk to Natural Hazards

Title: Quantifying Social Vulnerability: A Methodology for Identifying Those at Risk to Natural Hazards
Author(s): Dwyer, A., Zoppou, C., Nielson, O., Day, S. & Roberts, S.
Organization: Geoscience Australia and the Department of Industry, Tourism and Resources
Publisher: Geoscience Australia
Publishing Location: Australia
Edition: Unavailable
Pages: 101
Retrieved from: Geoscience Australia Record 2004/14
Hyperlink: http://www.ga.gov.au/image_cache/GA4267.pdf
Date of Publication: 2004

Description:

- "This report focuses on certain aspects of social vulnerability and its role in contributing to the risk from natural hazards. In particular, the study introduces a unique method of measuring the vulnerability of individuals within a household in order to contribute to the development of comprehensive natural hazard risk assessments." [p. v]
- The research undertaken for this report is driven by two needs:
  1. "To develop a custom-made methodology of quantifying social vulnerability that can be incorporated into the risk models being developed by the Risk Research Group at Geoscience Australia…
  2. Need to integrate social issues with hazard model development in order to investigate the greater risk to communities." [p. v]

Additional Information:
The methodology has four main steps:

1. Indicator selection
2. Risk Perception Questionnaire
3. Decision tree analysis
4. Synthetic Estimation

4.2.1.9 Comprehensive Risk Assessment for Natural Hazards

Title: Comprehensive Risk Assessment for Natural Hazards
Author(s): Charles S. Melching (U.S.A), Paul J. Pilon (Canada), Yadowsun Boodhoo (Mauritius), Renée Michaud (U.S.A), Laurent Stiltjes (France), Jean-Jacques Wagner (Switzerland), Dieter Mayer-Rosa (Switzerland), Olivier Lateltin (Switzerland), Christoph Bonnard (Switzerland)
Editors: Charles S. Melching (U.S.A), Paul J. Pilon (Canada)
Organization: World Meteorological Organization (WMO)
Publisher: World Meteorological Organization (WMO)
Publishing Location: Unavailable
Edition: 2nd ed. (Reprinted 2006; Original printed 1999)
Pages: 100
Retrieved from: WMO/TD No. 955, from the World Meteorological Organization website
Hyperlink:
http://www.wmo.int/pages/prog/drr/publications/drrPublications/TD0955_Comprehensive_Assessment_of_Natural_Hazards/WMO_TD0955e.pdf
Date of Publication: Reprinted 2006

Purpose:

- "The primary aim of this report is not to propose the development of new methodologies and technologies. The emphasis is rather on identifying and presenting the various existing technologies used to assess the risks for natural disasters of different origins and to encourage their application, as appropriate, to particular circumstances around the world. A very important aspect of this report is the promotion of comprehensive or joint assessment of risk from a variety of possible natural activities that could occur in a region. At the same time, it does identify gaps where there is a need for enhanced research and development. By presenting the technologies within one volume, it is possible to compare them, for the specialists from one discipline to learn from the practices of the other disciplines, and for the specialists to explore possibilities for joint or combined assessments in some regions." [p. vii]

Additional Information:
This report discusses the following:

- Meteorological hazards
- Hydrological hazards
- Volcanic hazards
- Seismic hazards
- Hazard assessment and land-use planning in Switzerland
- Vulnerability – Economic considerations
- Strategies for risk assessment - Case studies

4.2.2 Man-Made Unintentional Hazards

4.2.2.1 Integrating Manmade Hazards Into Mitigation Planning

**Note:* Since this guide considers both malicious and non-malicious manmade hazards, this reference would also be appropriate under section *4.3: Multi-Threats*.

Title: Integrating Manmade Hazards Into Mitigation Planning
Author(s): Federal Emergency Management Agency (FEMA)
Organization: Federal Emergency Management Agency (FEMA)
Publisher: Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: Version 2.0
Pages: 78
Retrieved from: FEMA Library website, publication number 386-7
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=1915
Date of Publication: September 2003

Purpose:

- "FEMA has developed this series of mitigation planning 'how-to' guides to assist states, communities and tribes in enhancing their hazard mitigation planning capabilities." [p. i]

Scope:

- These guides are applicable to states and communities of various sizes and varying ranges of financial and technical resources." [p. i]

Description:
"Although mitigation planning traditionally focused on planning for natural hazards, events such as the September 11, 2001 attacks, [and]the July 2001 Baltimore hazardous material train derailment[,] suggested that the time had come to incorporate terrorism and technological hazards into all aspects of emergency management planning, not just preparedness and response. In addition, the 1996 Olympic Park bombing, the 1995 destruction of the Murrah Federal Building in Oklahoma City, the 1993 World Trade Center bombing, and scores of smaller-scale incidents and accidents reinforced the need for communities to reduce their vulnerability to future terrorist acts and technological disasters. How-To Guide # 7 (FEMA 386-7) assumes that a community is engaged in the mitigation planning process and serves as a resource to help the community expand the scope of its plan to address terrorism and technological hazards. This Guide provides information to supplement the community's hazard mitigation planning efforts.[18]"

Additional Information:

- This document provides information that will assist users in incorporating manmade hazards into the hazard mitigation planning process. Thus, it guides the user through each of the 4 steps of the hazard mitigation planning process. They are:
  1. Organize resources
  2. Assess risks
  3. Develop a mitigation plan
  4. Implement the plan and monitor progress
- This guide includes worksheets and checklists to provide assistance through the process.

[18] From http://www.fema.gov/library/viewRecord.do?id=1915

4.2.2.2 An International Comparison of Four Quantitative Risk Assessment Approaches - Benchmark Study Based on a Fictitious LPG Plant

Title: An International Comparison of Four Quantitative Risk Assessment Approaches - Benchmark Study Based on a Fictitious LPG Plant
Author(s): National Institute for Public Health and the Environment, Ministry of Health, Welfare and Sport
Organization: National Institute for Public Health and the Environment
Publisher: Unavailable
Publishing Location: Netherlands
Edition: Unavailable
Pages: 158
Retrieved from: RIVM Report 620552001/2011
Hyperlink: http://www.rivm.nl/dsresource?objectid=rivmp:76359&type=org&disposition=inline
Date of Publication: 2011

Abstract:
"The methods to determine external safety risks used in the United Kingdom, France, the Walloon Region of Belgium and the Netherlands are very different. The differences concern both the way the calculations are performed and the consequences calculated (such as deaths or health damage to persons). Despite the differences, the methods yield similar results in terms of the safety distances. This conclusion can be drawn from a benchmark study of a fictitious LPG storage plant performed by experts of these countries. However, similar results can lead to different policy implications. For instance, the safety distances in the Netherlands and France are used as limit values, whereas in Belgium and the United Kingdom they are used as guide values." [p. 3]

Keywords: quantitative risk assessment, QRA, benchmark study, LPG, external safety

Note: The scenarios used for the benchmark study of a fictitious LPG storage plant are accidental.

4.2.3 Health Hazards

4.2.3.1 Federal Contaminated Site Risk Assessment in Canada - Part I: Guidance on Human Health Preliminary Quantitative Risk Assessment (PQRA)

Title: Federal Contaminated Site Risk Assessment in Canada - Part I: Guidance on Human Health Preliminary Quantitative Risk Assessment (PQRA)
Author(s): Environmental Health Assessment Services Division, Safe Environments Programme, Health Canada
Organization: Health Canada
Publisher: Health Canada
Publishing Location: Canada
Edition: Unavailable
Pages: 41
Retrieved from: Health Canada website
Hyperlink: http://www.hc-sc.gc.ca/ewh-semt/alt_formats/hecs-sesc/pdf/pubs/contamsite/part-partie_i/part-partie_i-eng.pdf
Date of Publication: September 2004

*Externally peer reviewed

Purpose:

- "The purpose of this guidance document is to prescribe, to the degree possible, standard exposure pathways, receptor characteristics, toxicological reference values, and other parameters required to quantitatively assess the potential chemical exposures and risks at federal contaminated sites." [p. 2]

Scope:

- "The standard PQRA approach presented herein is designed specifically for the assessment of sites that are to remain the properties of federal agencies, properties for which greater consistency in risk assessment methods and interpretation of results is required." [p. 3]

Additional Information:

- This guidance prescribes the content that should be included in the Preliminary Quantitative Risk Assessment Report. The steps covered are:
    - Description of the Property/Site
    - Problem Formulation
    - Exposure Assessment
    - Hazard Assessment
    - Risk Characterization
    - Non-Standard Assumptions and Toxicological Reference Values
    - Uncertainties
- The document also includes recommendations for equations, factors, values, and other parameters to be used in the risk assessment process, as well as explanations of why these methods are requested in the Preliminary Quantitative Risk Assessment Report.

4.2.3.2 Hazard Risk Assessment Instrument

Title: Hazard Risk Assessment Instrument
Author(s): UCLA (University of California, Los Angeles) Center for Public Health and Disasters
Organization: UCLA (University of California, Los Angeles) Center for Public Health and Disasters
Publisher: UCLA (University of California, Los Angeles) Center for Public Health and Disasters
Publishing Location: Los Angeles, California
Edition: 1st ed.
Pages: 89
Retrieved from: UCLA Center for Public Health and Disasters website
Hyperlink: http://www.cphd.ucla.edu/npdfs/HRAI_Workbook.pdf
Date of Publication: January 2006

Description:

- "The Hazard Risk Assessment Instrument (HRAI) workbook is intended to be used as a guide to enable state and local public health agencies to conduct a risk assessment of their community. The tool is designed for use as a standard approach to hazard risk assessment that is adapted to the public health impacts of hazards. HRAI will allow public health agencies to assess the probability of hazards for a particular geographic area and the magnitude of impact given the local resources, allowing for prioritization of response and mitigation options. As such, this workbook will guide public health agencies in determining the likelihood of a hazard occurring, assessing their community's vulnerabilities and current resources, and prioritizing resources in planning for disasters.
- This instrument is based on the expertise of the authors and incorporates disaster-related data in order to illustrate its systematic methodology.
- This workbook may not be inclusive of all the parameters pertinent to a specific jurisdiction. Therefore, it is the responsibility of the user to research local procedures and laws to ensure validity of the final product." [Disclaimer]

Additional Information:

- The Hazard Risk Assessment Instrument (HRAI) consists of four steps. They are:
  1. Probability of Mishap
  2. Severity of Consequences
  3. Scoring the Consequences
  4. Risk Analysis
- The HRAI provides step-by-step guidance for each of the above steps. It provides worksheets, indicators, scoring guidelines, and examples in order to assist users.

4.2.3.3 Concepts, Methods, and Data Sources for Cumulative Health Risk Assessment of Multiple Chemicals, Exposures and Effects: A Resource Document (Final Report)

Title: Concepts, Methods, and Data Sources for Cumulative Health Risk Assessment of Multiple Chemicals, Exposures and Effects: A Resource Document (Final Report)
Author(s): Environmental Protection Agency, National Center for Environmental Assessment - Cincinnati Division (NCEA)
Organization: U.S. Environmental Protection Agency
Publisher: U.S. Environmental Protection Agency
Publishing Location: Cincinnati, OH
Edition: Unavailable
Pages: 412
Retrieved from: EPA/600/R-06/013F
Hyperlink: N/A
Date of Publication: August 2007

*Subjected to the Agency's peer and administrative review

Abstract:
"Public interest in the health impacts of environmental chemical exposures and their interactions with other stressors continues to grow with increased information about exposures to multiple chemicals in air, water and soil from different sources. However, population vulnerability factors, such as diet, behaviors, genetic traits, economic status and social characteristics are often not considered. Cumulative risk assessment may be thought of as a population-based analysis, characterization and possible quantification of the combined risks to health or the environment from multiple route exposures to multiple agents or stressors. This current report serves as a resource document for identifying specific elements of and approaches for implementing cumulative risk assessments. This report is not a regulatory document and is not guidance but rather a presentation of concepts, methods and data sources. It is designed to assist EPA's development of specific approaches and cumulative risk guidance for use by its Program Offices and Regions. It is intended as a resource for EPA scientists and others in the broader risk assessment community with an interest in locating data and approaches relevant to cumulative risk assessment. This report focuses on two areas: initiating factors for a cumulative risk assessment with procedures for data collection and organization; and technical approaches for assessing and characterizing human health risks associated with a subset of cumulative risk issues (i.e., multiple chemicals, exposures and effects). Schematics are shown for evaluating data, profiling the population of concern, grouping chemicals into integrated exposure and toxicity groups, performing toxicity assessments and conducting cumulative risk characterizations. Issues discussed include toxicological interactions, pharmacokinetics, multiple toxic effects, epidemiologic methods, biomonitoring data, the temporal nature of exposures and environmental chemical transformations. Articulation of variability and uncertainty is stressed as part of the final Risk Characterization." [p. ii]

4.2.3.4 Assessing the Risk from Emerging Infections

Title: Assessing the Risk from Emerging Infections
Author(s): D. Morgan, H. Kirkbride, K. Hewitt, B. Said and A.L. Walsh
Organization: Department of Gastrointestinal, Emerging and Zoonotic Infections, Health Protection Agency Centre for Infections, London, UK
Publisher: Cambridge University Press
Publishing Location: United Kingdom
Edition: N/A
Pages: 1521-1530
Retrieved from: Epidemiology and Infection, vol. 137, no. 11
Hyperlink: N/A
Date of Publication: November 2009

Abstract:
"Emerging infections pose a constant threat to society and can require a substantial response, thus systems to assess the threat level and inform prioritization of resources are essential. A systematic approach to assessing the risk from emerging infections to public health in the UK has been developed. This qualitative assessment of risk is performed using algorithms to consider the probability of an infection entering the UK population, and its potential impact, and to identify knowledge gaps. The risk assessments are carried out by a multidisciplinary, cross-governmental group of experts working in human and animal health. This approach has been piloted on a range of infectious threats identified by horizon scanning activities. A formal risk assessment of this nature should be considered for any new or emerging infection in humans or animals, unless there is good evidence that the infection is neither a recognized human disease nor a potential zoonosis." [p. 1521]

Key words: Emerging infections; infectious disease epidemiology; public health; risk assessment; zoonoses.

Purpose:
- "The purpose of this work was to develop a rapid, systematic, objective and transparent method for assessing the risk to the UK population from new and emerging infections arising anywhere in the world." [p. 1522]

Additional Information:
This document includes:
- Brief review of two previous works on risk assessment in order to define best practice and consistency of approach
  - HPZone: by the Department of Health (England)
  - Risk assessment model by the Department for the Environment and Rural Affairs
- Description of the development of a risk assessment tool based on the findings from these two projects
- Illustration of the risk assessment tool through an example: the Chikungunya infection

4.2.3.5 Documentation for Prototype AHW Prioritisation Decision Support Tool

Title: Documentation for Prototype AHW Prioritisation Decision Support Tool
Author(s): Surveillance, Zoonoses and Emerging Issues Division (SZEID), Department for Environment, Food and Rural Affairs (DEFRA)
Organization: Department for Environment, Food and Rural Affairs (DEFRA)
Publisher: Department for Environment, Food and Rural Affairs (DEFRA)
Publishing Location: London, UK
Edition: Unavailable
Pages: 14
Retrieved from: DEFRA archive
Hyperlink:
http://archive.defra.gov.uk/foodfarm/farmanimal/diseases/vetsurveillance/documents/dst_summary.pdf
Date of Publication: December 2006

Description:

- "The tool aims to provide an evidence based foundation on which decisions on resource allocation can be made through dialogue and negotiation. It calculates, for each disease/issue considered, a score for the risk and impact on each of four 'reasons for interventions' derived from up to 10 key criteria that have been identified and defined with wide stakeholder input. The prototype tool is transparent and understandable to anyone with basic Excel skills.
- This document describes the prototype tool itself, and defines the criteria and proposed categorical score options and weighting to be used in the exploration of the process for using such a tool." [p. 1]

4.2.3.6 HPZone Risk Assessment

Title: HPZone Risk Assessment
Author(s): Unavailable
Organization: Unavailable
Publisher: N/A
Publishing Location: N/A
Edition: Unavailable
Pages: N/A
Retrieved from: HPZone website
Hyperlink: http://hpzoneinfo.in-fact.com/
Date of Publication: Unavailable

Description:

- This website provides an overview of HPZone's risk assessment model.
- This model "was developed over a three year period and validated across the UK. The model has demonstrated improved efficiency and effectiveness of management of outbreaks.
- The model consists of five attributes rated over a 0 to 4 scale. The attributes are severity, spread, uncertainty in the diagnosis, ease of intervention and the wider context in which events are occurring. During the outbreak, the dynamic risk assessment of each event occurring is used to inform management action at that time.[19]"

[19] From http://hpzoneinfo.in-fact.com/

4.2.3.7 Operational Guidance on Rapid Risk Assessment Methodology

Title: Operational Guidance on Rapid Risk Assessment Methodology
Author(s): Dilys Morgan, Hilary Kirkbride and Bengü Said (Health Protection Agency UK)
Organization: European Centre for Disease Prevention and Control
Publisher: European Centre for Disease Prevention and Control
Publishing Location: Stockholm, Sweden
Edition: Unavailable
Pages: 73
Retrieved from: European Centre for Disease Prevention and Control, Technical Document
Hyperlink:
http://www.ecdc.europa.eu/en/publications/Publications/1108_TED_Risk_Assessment_Methodology_Guidance.pdf
Date of Publication: August 2011

Purpose:

- "The aim of this guidance is to define rapid risk assessment methodology, indicating where there are the existing elements which could be applied to producing a rapid risk assessment and where there need to be new approaches.
- The main objective is to develop an operational tool to facilitate rapid risk assessments for communicable disease incidents, drawing on the systematic methods used in evidence-based medicine or evidence-based practice where possible...
- The operational guidance will support the use of a common defined methodology." [p. 2]

Audience:

- "National public health experts within Member States and experts responsible for rapid assessment of communicable disease threats at the European level." [p. 2]

Description:

- "This guidance document develops a methodology for rapid risk assessments undertaken in the initial stages of an event or incident of potential public health concern. It describes an operational tool to facilitate rapid risk assessments for communicable disease incidents at both Member State and European level. The tool comprises information tables and risk-ranking algorithms to give an estimate of risk posed by a threat." [p. v]
- The operational guidance tool has been tested.

Additional Information:
This guidance "outlines the process of undertaking a rapid risk assessment, including the approach to, and tools required at, each step of the process." [p. 5]
They are:

- "Stage 0: Preparation
- Stage 1: Collect event information
- Stage 2: Perform a structured literature search/systematically collecting formation about the (potential) aetiologic agent
- Stage 3: Extract relevant evidence
- Stage 4: Appraise evidence
- Stage 5: Estimate risk" [p. 5]

4.2.3.8 Risk and Risk Assessment in Health Emergency Management (Theoretical Discussion)

Title: Risk and Risk Assessment in Health Emergency Management (Theoretical Discussion)
Author(s): Jeffrey L. Arnold, MD
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 143-154
Retrieved from: Prehospital and Disaster Medicine, Vol. 20, No. 3
Hyperlink: http://pdm.medicine.wisc.edu/Volume_20/issue_3/arnold.pdf
Date of Publication: May-June 2005

Abstract:

"This article considers the critical roles of risk and risk assessment in the management of health emergencies and disasters. The Task Force on Quality Control of Disaster Management (TFQCDM) has defined risk as the "objective (mathematical) or subjective (inductive) probability that something negative will occur (happen)". Risks with the greatest relevance to health emergency management include: (1) the probability that a health hazard exists or will occur; (2) the probability that the hazard will become an event; (3) the probability that the event will lead to health damage; and (4) the probability that the health damage will lead to a health disaster. The overall risk of a health disaster is the product of these four probabilities.

Risk assessments are the tools that help systems at risk—healthcare organizations, communities, regions, states, and countries—transform their visceral reactions to threats into rational strategies for risk reduction. Type I errors in risk assessment occur when situations are predicted that do not occur (risk is overestimated). Type II errors in risk assessment occur when situations are not predicted that do occur (risk is underestimated). Both types of error may have serious, even lethal, consequences.

Errors in risk assessment may be reduced through strategies that optimize risk assessment, including the: (1) adoption of the TFQCDM definition of risk and other terms; (2) specification of the system at risk and situations of interest (hazard, event, damage, and health disaster); (3) adoption of a best practice approach to risk assessment methodology; (4) assembly of the requisite range of expert participants and information; (5) adoption of an evidence-based approach to using information; (6) exclusion of biased, irrelevant, and obsolete information; and (7) complete characterizations of any underlying fault and event trees." [p. 143]

Keywords: definition; disaster; disaster medicine; emergency; emergency management; error; event; evidence; evidence-based medicine; harmonization; hazard; health; risk; risk assessment; risk assessment matrix; risk characterization; risk management; terrorism; vulnerability

Additional Information:
This paper includes:

- Description of risk, risk assessments, and risk management
- Discussion on identifying and reducing errors in risk assessments
- Suggestions for optimizing the risk assessment process

4.2.3.9 Measuring the Uncertainties of Pandemic Influenza

Title: Measuring the Uncertainties of Pandemic Influenza
Author(s): Jeanne Fair, Dennis Powell, Rene Le Claire, Leslie Moore, Michael Wilson, Lori Dauelsberg, Michael Samsa, Gary Hirsch, Brian Bush
Organization: N/A
Publisher: Inderscience Publishers
Publishing Location: Unavailable
Edition: N/A
Pages: Unavailable
Retrieved from: International Journal of Risk Assessment and Management (IJRAM)
Hyperlink: http://www.inderscience.com/info/inarticle.php?artid=47550
Date of Publication: In Press

Abstract:
"It has become critical to assess the potential range of consequences of a pandemic influenza outbreak given the uncertainty about its disease characteristics, while investigating risks and mitigation strategies of vaccines, antivirals, and social distancing measures. Here, we use a simulation model and rigorous experimental design with sensitivity analysis that incorporates uncertainty in the pathogen behaviour and epidemic response to show the extreme variation in the consequences of a potential pandemic outbreak in the United States. Using sensitivity analysis, we found the most important disease characteristics are the fraction of the transmission that occur prior to symptoms, the reproductive number, and the length of each disease stage. Using data from the historical pandemics and for potential viral evolution, we show that response planning may underestimate the pandemic consequences by a factor of two or more.[20]"

Keywords: influenza; epidemics; public health epidemiology; pandemic

[20]From http://www.inderscience.com/info/inarticle.php?artid=47550

4.2.4 Multi-Hazard

4.2.4.1 Multi-Hazard Identification and Risk Assessment: A Cornerstone of the National Mitigation Strategy

Title: Multi-Hazard Identification and Risk Assessment: A Cornerstone of the National Mitigation Strategy
Author(s): Federal Emergency Management Agency's (FEMA) Mitigation Directorate
Organization: Federal Emergency Management Agency (FEMA)
Publisher: Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: 1st ed.
Pages: 369
Retrieved from: FEMA Resource Library website
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=2214
Date of Publication: 1997

Purpose:

- "This report is intended to serve as a baseline for hazard identification and risk assessment efforts. The research and reviews documented in this report are not intended to be exhaustive evaluations of hazards and the risks they pose throughout the United States...
- FEMA initiated this report to focus primarily on identification of hazards and factors important to risk assessment: probability and frequency, exposure, and consequences." [p. xxv]

Scope:

- This report covers two types of hazards: natural hazards and technological hazards.

Description:

- For each of the hazards discussed, this report "summarizes the state of scientific and technical knowledge on identification and the risks that have been or can be assigned to each hazard." [p. xvii]
- This document also discusses various risk assessment approaches, and introduces FEMA's risk assessment methodology, Hazards United States (HAZUS).
- In addition, it summarizes the National Mitigation strategy and highlights recent successes in each of the 5 major elements of the strategy. They are:
    - "Hazard identification and risk assessment
    - Applied research and technology transfer
    - Public Awareness, training, and education
    - Incentives and resources
    - Leadership and coordination." [p. xvii]

4.2.4.2 A Methodological Approach for the Definition of Multi-Risk Maps at Regional Level: First Application

Title: A Methodological Approach for the Definition of Multi-Risk Maps at Regional Level: First application
Author(s): A. Carpignano, E. Golia, C. Di Mauro, S. Bouchon and J-P. Nordvik
Organization: N/A
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 513-534
Retrieved from: Journal of Risk Research, Vol. 12, Nos. 3-4
Hyperlink: N/A
Date of Publication: April-June 2009

Abstract:
"Technological and natural disasters occurred in Europe during last decades showed an increased vulnerability of our society to different risks. Authorities and civil protection need instruments which allow having a better understanding of the variety of risks over a territory and help them in managing the resources and planning the emergency. However, many difficulties arise in comparing hazards, vulnerabilities and risks among them. The existing risk mapping in European countries often allows a simplified comparison of risks by means of potential damages but does not permit any qualitative assessment of multi-risk situations.

The aim of this project carried out for the Piedmont Region (Italy) is the development of a decision support system based on a multi-risk approach which can overcome difficulties in the overall risk assessment over a territory. To define multi-risk maps, a multi-risk perspective and stakeholder's perceptions were integrated to a classical risk assessment frame.
The specific purpose of this work is describing the methodological framework built up at this stage of the project and discussing the first results." [p. 513]

Keywords: territory; risk-management; multi-risk; maps; decision support instrument

Description:
This paper includes:

- Emphasis on the value of the multi-risk approach
- Discussion of the issues and limitations of the multi-risk approach
- Analysis of the multi-risk situation in Europe, as well as a discussion on the benefits and limitations of existing multi-risk mapping practices
- Presentation of the methodology developed for the Piedmont region research, as well as an overview of the first results

4.2.4.3 A Methodology for an Integrated Risk Assessment of Spatially Relevant Hazards

Title: A Methodology for an Integrated Risk Assessment of Spatially Relevant Hazards
Author(s): Stefan Greiving; Mark Fleischhauer; Johannes Lückenkötter
Organization: N/A
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 1-19
Retrieved from: Journal of Environmental Planning and Management, vol. 49, no. 1
Hyperlink: http://www.plan-risk-consult.de/wp-content/uploads/2008/05/lr_119_jepm_risk_methodology.pdf
Date of Publication: January 2006

Abstract:
"Natural and technological disasters of the past have shown that such incidences significantly affect local and regional development. Faced with the task of ensuring economic, human and environmental development as well as insuring physical structures, planning authorities, insurance companies and emergency managers are looking for methodologies to identify highly sensitive areas in terms of their overall risk. Existing methodologies like the Natural Hazard Index for Megacities or the Total Place Vulnerability Index have limitations due to their sectoral approach, which makes them less useful for integrated spatial planning. This paper presents the Integrated Risk Assessment of Multi-Hazards as a new approach to serve as a basis for a spatial risk management process. The approach integrates various hazards into an integrated hazard map, combines this with the region's vulnerability and thus produces an integrated risk map. Moreover, the methodology offers a tool to derive weighting factors for hazards as well as for vulnerability components." [p. 1]

Purpose:

- "The goal of this risk assessment approach is to determine the total risk potential of a sub-national region. This means aggregating all relevant risks... to arrive at an integrated risk potential." [p. 12]

Scope:

- "In principle the methodology can be applied at any geographical level and for any hazard and risk related purpose." [p. 12]

4.2.4.4 An Overview of Quantitative Risk Measures for Loss of Life and Economic Damage

Title: An Overview of Quantitative Risk Measures for Loss of Life and Economic Damage
Author(s): S.N. Jonkman, P.H.A.J.M. van Gelder, J.K. Vrijling
Organization: N/A
Publisher: Elsevier
Publishing Location: Amsterdam, Netherlands
Edition: N/A
Pages: 1-30
Retrieved from: Journal of Hazardous Materials, Vol. 99, No. 1
Hyperlink: N/A
Date of Publication: April 4, 2003

Abstract:
"A comprehensive overview of methods to quantify and limit risks arising from different sources is still missing in literature. Therefore, a study of risk literature was carried out by the authors. This article summarises about 25 quantitative risk measures. A risk measure is defined as a mathematical function of the probability of an event and the consequences of that event. The article focuses mainly on risk measures for loss of life (individual and societal risk) and economic risk, concentrating on risk measurement experiences in The Netherlands. Other types of consequences and some international practices are also considered. For every risk measure the most important characteristics are given: the mathematical formulation, the field of application and the standard set in this field. Some of the measures have been used in a case study to calculate the flood risks for an area in The Netherlands." [p. 1]

Additional information:
This paper covers the following topics:

- Risk Measures, categorized according to the consequences that they consider. They are:
  - Fatalities - Individual Risk
  - Fatalities - Societal Risk
  - Economic Damage
  - Environmental damage
  - Potential Damage
  - Integrated risk measures: considering various types of consequences
- Summary of available methods for the monetary valuation of human life
- Case study: Calculation of flood risks for an area in the Netherlands, using some of the above measures
- Summary chart of risk measures
- Evaluation of important aspects

4.3 Malicious Threats

4.3.1 Cyber Threats

4.3.1.1 Automated Risk Management System

Title: Automated Risk Management System
Author(s): Glen Henderson, Reginald Sawilla, Stan Matwin, Eugen Bacic, Larry Tremblay, Jelber Sayyad-Shirabad, Erico N. de Souza
Organization: Defence R&D Canada (DRDC) - Ottawa
Publisher: Defence R&D Canada (DRDC) - Ottawa
Publishing Location: Ottawa, Canada
Edition: Unavailable
Pages: 140
Retrieved from: DRDC - Ottawa, Technical Report (DRDC Ottawa TR 2012-060)
Hyperlink: N/A
Date of Publication: May 2012

Abstract:
"Communications and Information Technology is identified by Public Safety Canada as one of the ten critical infrastructure sectors. This sector in particular, and all critical infrastructure sectors in general, are heavily reliant upon information technology systems for operations, planning, communication, logistics, command, and control. Effective service provision, disaster planning, and disaster recovery all require a comprehensive understanding of the system-wide cascading impacts of a security incident. Cascading effects not only significantly broaden the impact of a single incident but can also trigger new events involving other infrastructure services. The problem is particularly challenging for information technology networks since, in addition to the dynamically changing operational priorities germane to all networks, one must also consider the dynamicity of the network itself.

We discuss methods to consistently and, where possible, automatically capture interdependencies from governance to business services to infrastructure to physical location. Risk management methodologies are reviewed for their applicability to an automated system. Existing technologies for computing quantitative criticality metrics are reviewed in relation to their ability to respond to changing business needs and infrastructure. These foundational elements enable course of action planning to reduce and mitigate risks, while considering cascading impacts. High-level design and requirements are proposed for an automated risk management system to assist planners in making informed risk management decisions." [p. i]

Description:
- "We propose an approach to achieve an Automated Risk Management System (ARMS) that is capable of discovering dependencies in Information Technology (IT) systems and analyzing the systems in order to enable system planners and response agents to make informed risk management decisions on system design and configuration." [p. iii]

4.3.1.2 Harmonized Threat and Risk Assessment (TRA) Methodology

Title: Harmonized Threat and Risk Assessment (TRA) Methodology
Author(s): Communications Security Establishment and the Royal Canadian Mounted Police
Organization: Communications Security Establishment and the Royal Canadian Mounted Police
Publisher: Unavailable
Publishing Location: Canada
Edition: Unavailable
Pages: 290
Retrieved from: Communications Security Establishment Canada website
Hyperlink: http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf
Date of Publication: October 23, 2007

Purpose:

- This document presents the *Harmonized Threat and Risk Assessment Methodology,* and is intended to serve as a comprehensive toolkit for departmental risk managers.

Description:

- The Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP) published technical documents with the aim of assisting government institutions in conducting the threat and risk assessment. Despite these efforts, many challenges remained, and the CSE and the RCMP initiated a joint project to develop a single *Harmonized Threat and Risk Assessment Methodology* for the government of Canada.

Additional Information:
"Major modules of the Harmonized Threat and Risk Assessment Methodology include:

- a Foreword to identify the authority for issuing the document and provide a point of contact for questions and suggested improvements, as well as the usual Table of Contents and Lists of Figures and Tables;
- an Executive Overview to explain the importance of TRAs as a tool to help senior executives meet their responsibilities and accountabilities for Modern Comptrollership, and the Integrated Risk Management and Management Accountability Frameworks;
- an Introduction to review some background, the rationale for a new methodology, the objectives and principles that governed its development, and the structure adopted to achieve these goals;
- a Management Summary to describe the entire TRA process at a high level for program and project managers with risk management responsibilities;
- a series of six Annexes to present each step of the TRA process in greater detail for program, project and security staff who must apply the methodology in practice;
- an array of Appendices with even more detailed material in the form of diagrams, technical descriptions, checklists, flowcharts, tables, and templates to illustrate every aspect of the TRA process and facilitate easy application; and
- a seventh Annex containing additional supporting material, such as a comprehensive Glossary, List of Acronyms and References." [p. 3]

4.3.1.3 A Risk-Assessment Model for Cyber Attacks on Information Systems

Title: A Risk-Assessment Model for Cyber Attacks on Information Systems
Author(s): Sandip Patel, Jigish Zaveri
Organization: Department of Information Science & Systems, Morgan State University
Publisher: Academy Publisher
Publishing Location: Unavailable
Edition: N/A
Pages: 352-359
Retrieved from: Journal of Computers, Vol. 5, No. 3
Hyperlink: N/A
Date of Publication: March 2010

Abstract

"Industrial process-plants are an integral part of a nation's economy and critical infrastructure. The information systems used by automated industrial plants are enticing targets of cyber attacks. However, the financial damages resulting from these cyber attacks are difficult to estimate since the resultant losses are not as tangible as physical losses. In this paper, we propose a mathematical model for determining the financial losses resulting from cyber attacks on a computer-based information system used in industrial plants.

Limited work has been published to systematically explore the types of possible cyber attacks and their financial impact on the process. The primary objective of this research is to propose a risk-assessment model to assess the impact of cyber attacks on a plant that runs fully or partially by control systems such as supervisory control and data acquisition (SCADA). Managers could use the model for cost/benefit analysis of security software and hardware acquisition. We also illustrate this model's use on a SCADA system using a case. The proposed model could be applied to different industries and organizations with minor modifications to reflect the specifics of that industry or organization." [p. 352]

Key words: Cyber attacks; computer security; risk assessment; control systems; information systems

4.3.1.4 Principles for Better Information Security through More Accurate, Transparent Risk Scoring

Title: Principles for Better Information Security through More Accurate, Transparent Risk Scoring
Author(s): Kenneth G. Crowther, Yacov Y. Haimes, M. Eric Johnson
Organization: N/A
Publisher: Berkeley Electronic Press
Publishing Location: Unavailable
Edition: N/A
Pages:1-18
Retrieved from: Journal of Homeland Security and Emergency Management, Vol. 7, Issue 1, Article 37
Hyperlink: N/A
Date of Publication: 2010

Abstract:
"This paper explores approaches for scoring information security risk that could lead to investment drivers and drive appropriate levels of security. Our approach is grounded on two important factors that determine cyber risk: (1) the information security resources (e.g., technologies, skills, and policies) that reduce the likelihood and consequences of successful information exploits; and (2) the security processes and capabilities that drive a continuous improvement of the security resources in use. The quality of a cyber defense system is the result of the integration of these two factors. This manuscript proposes such a two-factor hierarchical system of scoring, details candidate measures, and explores economic conditions for selecting appropriate measures. We review several scoring systems available that contain elements from this proposed system and discuss conditions for market adoption of information security scoring.[21]"

Key words: risk scoring; cyber security; information security; vulnerability; resilience

[21] From http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1658/jhsem.2010.7.1.1658.xml

4.3.1.5 Coupled Petri Nets for Computer Network Risk Analysis

Title: Coupled Petri Nets for Computer Network Risk Analysis
Author(s): Matthew H. Henry, Ryan M. Layer, David R. Zaret
Organization: N/A
Publisher: Elsevier Ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 67-75
Retrieved from: International Journal of Critical Infrastructure Protection, Vol. 3, No. 2
Hyperlink: N/A
Date of Publication: July 2010

Abstract
"This paper presents a framework for quantifying the risk induced by the potential for cyber attacks levied against network-supported operations. It also permits a formal assessment of candidate risk management policies that address network host vulnerabilities and host-process coupling. The framework incorporates a novel application of Petri net state coverability analysis coupled with process failure mode analysis. It extends previous work on Petri nets for attack analysis in three ways: (i) new metrics that quantify risk as a function of Petri net state and techniques for evaluating the metrics based on the minimal coverability set of a Petri net; (ii) a new method for coupling a Petri net representation of a computer network attack to a process failure modes model; and (iii) a new method for identifying high-value risk management opportunities. The paper concludes by presenting an application of the analysis techniques to evaluate risk in process control networks." [p. 67]

4.3.1.6 A Comprehensive Network Security Risk Model for Process Control Networks

Title: A Comprehensive Network Security Risk Model for Process Control Networks
Author(s): Matthew H. Henry and Yacov Y. Haimes
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 223-248
Retrieved from: Risk Analysis, Vol. 29, No. 2
Hyperlink: N/A
Date of Publication: February 2009

Abstract:
"The risk of cyber attacks on process control networks (PCN) is receiving significant attention due to the potentially catastrophic extent to which PCN failures can damage the infrastructures and commodity flows that they support. Risk management addresses the coupled problems of (1) reducing the likelihood that cyber attacks would succeed in disrupting PCN operation and (2) reducing the severity of consequences in the event of PCN failure or manipulation. The Network Security Risk Model (NSRM) developed in this article provides a means of evaluating the efficacy of candidate risk management policies by modeling the baseline risk and assessing expectations of risk after the implementation of candidate measures. Where existing risk models fall short of providing adequate insight into the efficacy of candidate risk management policies due to shortcomings in their structure or formulation, the NSRM provides model structure and an associated modeling methodology that captures the relevant dynamics of cyber attacks on PCN for risk analysis. This article develops the NSRM in detail in the context of an illustrative example." [p. 223]

Key words: Cyber attack modeling; network security; risk assessment

4.3.1.7 Security Risk Analysis Based on Probability of System Failure, Attacks and Vulnerabilities

Title: Security Risk Analysis Based on Probability of System Failure, Attacks and Vulnerabilities
Author(s): Dr. Ghassan Kbar (Associate Professor of IT, American University in Dubai (AUD), UAE)
Organization: Institute of Electrical and Electronics Engineers (IEEE), Arab Computer Society (ACS)
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 874-879
Retrieved from: Conference Proceedings, IEEE/ACS International Conference on Computer Systems and Applications, 2009
Hyperlink: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5069434
Date of Publication: 2009

Abstract:
"Network security management plays a crucial role in protecting organization assets and its computer infrastructure. This can be done by identifying the vulnerabilities and developing effective control that reduces the risk of attacks and failures. Network risk assessment is a subjective process that is linked to multiple variables. These variables are associated with the organization assets and their impact on the health of the organization. To preserve the value of these assets, they must be protected from failure or attacks. In addition vulnerability assessment must be undertaken to assess the value of these assets for possible deficiency that would cause successful attacks. The main factors affecting failure are possible of system failure, threats which can be related to internal and external attacks, environmental threat, and process related threats. A risk management methodology is described in this paper to assist managers in evaluating the security risk of their organization**.** This risk is based on multiple variables that are related to vulnerabilities, probability of failure, and possible attacks caused by threats." [p. 874]

4.3.1.8 Process Control System Security Technical Risk Assessment Methodology & Technical Implementation

Title: Process Control System Security Technical Risk Assessment Methodology & Technical Implementation
Author(s): Peter Kertzner, Jim Watters, Deborah Bodeau, Adam Hahn
Organization: Institute for Information Infrastructure Protection
Publisher: Unavailable
Publishing Location: Unavailable
Edition: 2nd ed.
Pages: 47
Retrieved from: Institute for Information Infrastructure Protection (I3P) Research Report, No. 13
Hyperlink: http://www.thei3p.org/docs/publications/ResearchReport13.pdf
Date of Publication: March 2008

Audience:

1. "The risk assessment team who must gather the data at the lowest levels and translate it into a form meaningful to corporate officers
2. The corporate officers who must understand and have confidence in the means used to obtain and present the information to them" [p. i]

Description:

- "This research report describes an approach to PCS [process control systems] technical security risk assessment that facilitates effective risk communication. This document describes a process that focuses on the methodical assessment of cyber security risk as it relates to an organization's primary business objectives." [p. i]
- "The Risk-to-Mission Assessment Process (RiskMAP) is methodical in that it decomposes a selected set of business objectives into their constituent activities and then links those activities to potential sources of risk in data processing and control components of an underlying PCS. The process creates as an artefact a multi-level relational matrix that records linkages between vulnerabilities in PCS network components and the business activities in which exploited vulnerabilities could find their expression. This matrix, in essence, serves as a model of an organization's business functions and the possible risks individual business objectives face due to underlying process control system vulnerabilities. The vulnerability of a PCS network node, when considered with a derived, node-level measure of business value, can be interpreted as a risk measure for business activities that rely on the availability and proper functioning of that node. Adverse impacts to business activities is a concern of top management and the self-archival nature of RiskMAP makes available for inspection the analysis supporting, and rationale behind, conclusions reached regarding an organization's exposure to risk." [p. iii]

4.3.1.9 A Markov Game Theory-Based Risk Assessment Model for Network Information System

Title: A Markov Game Theory-Based Risk Assessment Model for Network Information System
Author(s): Cui Xiaolin, Tan Xiaobin, Zhang Yong, Xi Hongsheng
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 1057-1061
Retrieved from: Conference Publications, Vol. 3, 2008 International Conference on Computer Science and Software Engineering
Hyperlink: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4722524
Date of Publication: 2008

Abstract:
"Risk assessment is a very important tool to acquire a present and future security status of the network information system. Many risk assessment approaches consider the present system security status, while the future security status, which also has an impact on assessing the system risk, is not taken into consideration. In this paper we propose a novel risk assessment model based on Markov game theory. In this model, all of the possible risk in the future will impact on the present risk assessment. The farther away from now, the smaller impact on the risk assessment it has. After acquiring the system security status, we proposed an automatic generated reinforcement scheme which will provide a great convenience to the system administrator. A software tool is developed to demonstrate the performance of the risk assessment of a network information system and a simulation example shows the effectiveness of the proposed model." [p. 1057]

Additional Information:
This paper includes sections on:

- Discussion on related work
- Framework for risk assessment
- Markov game theory-based risk assessment model
- Experiments and discussions
- Conclusions

4.3.1.10 Cyber Security Risk Assessment for SCADA and DCS Networks

Title: Cyber Security Risk Assessment for SCADA and DCS Networks
Author(s): P.A.S. Ralston, J.H. Graham, J.L. Hieb
Organization: N/A
Publisher: Elsevier
Publishing Location: Unavailable
Edition: Unavailable
Pages: 583-594
Retrieved from: ISA Transactions, Vol. 46, Issue 4
Hyperlink: N/A
Date of Publication: October 2007

Abstract
"The growing dependence of critical infrastructures and industrial automation on interconnected physical and cyber-based control systems has resulted in a growing and previously unforeseen cyber security threat to supervisory control and data acquisition (SCADA) and distributed control systems (DCSs). It is critical that engineers and managers understand these issues and know how to locate the information they need. This paper provides a broad overview of cyber security and risk assessment for SCADA and DCS, introduces the main industry organizations and government groups working in this area, and gives a comprehensive review of the literature to date. Major concepts related to the risk assessment methods are introduced with references cited for more detail. Included are risk assessment methods such as HHM, IIM, and RFRM which have been applied successfully to SCADA systems with many interdependencies and have highlighted the need for quantifiable metrics. Presented in broad terms is probability risk analysis (PRA) which includes methods such as FTA, ETA, and FEMA. The paper concludes with a general discussion of two recent methods (one based on compromise graphs and one on augmented vulnerability trees) that quantitatively determine the probability of an attack, the impact of the attack, and the reduction in risk associated with a particular countermeasure." [p. 583]

4.3.1.11 Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology

Title: Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology
Author(s): Gary Stoneburner, Alice Goguen, and Alexis Feringa
Organization: Information Technology Laboratory (ITL), National Institute of Standards and Technology
Publisher: National Institute of Standards and Technology
Publishing Location: Gaithesburg, MD
Edition: N/A
Pages: 54
Retrieved from: National Institute of Standards and Technology Special Publication 800-30
Hyperlink: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Date of Publication: July 2002

Purpose:

- "This guide provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.
- In addition, this guide provides information on the selection of cost-effective security controls. These controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information." [p. 1-2]

Audience:

- "Federal organizations which process sensitive information." [p. 1]
- More specifically, this guide "provides a common foundation for experienced and inexperienced, technical, and non-technical personnel who support or use the risk management process for their IT systems." [p. 2]

Additional Information:
This guide is divided into the following sections:

- “Section 2 provides an overview of risk management, how it fits into the system development life cycle (SDLC), and the roles of individuals who support and use this process.
- Section 3 describes the risk assessment methodology and the nine primary steps in conducting a risk assessment of an IT system.
- Section 4 describes the risk mitigation process, including risk mitigation options and strategy, approach for control implementation, control categories, cost-benefit analysis, and residual risk.
- Section 5 discusses the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.” [p. 3]
- The appendices provide samples to assist the process of risk management, as well as a list of acronyms, a glossary of terms, and references.

4.3.1.12 A Qualitative Risk Analysis and Management Tool - CRAMM

Title: A Qualitative Risk Analysis and Management Tool - CRAMM
Author(s): Zeki Yazar
Organization: SANS Institute
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Version 1.3
Pages: 15
Retrieved from: SANS Institute Reading Room site
Hyperlink: http://www.sans.org/reading_room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm_83
Date of Publication: 2002

Abstract:
"Facing the emerging challenges of the Internet era, managers and information security professionals in business and government should manage specific risks to their organizations to ensure efficient operations. This paper explains basic components of risk analysis and management processes and mentions different methodologies and approaches. It then describes and discusses CRAMM, as an automated tool based on qualitative risk assessment methodology, by going through the stages of a CRAMM review, i.e. asset identification and valuation, threat and vulnerability assessment, and countermeasure recommendation. Raising organizational awareness CRAMM is a comprehensive and flexible tool especially for justifying prioritized countermeasures at a managerial level, needing, however, qualified and experienced practitioners for efficient results." [p. 1]

4.3.1.13 Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements

Title: Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements
Author(s): Sandip C. Patel, James H. Graham, Patricia A.S. Ralston
Organization: N/A
Publisher: Elsevier Ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 483-491
Retrieved from: International Journal of Information Management, Vol. 28, No. 6
Hyperlink: N/A
Date of Publication: December 2008

Abstract:

"This paper proposes a new approach for assessing the organization's vulnerability to information-security breaches. Although much research has been done on qualitative approaches, the literature on numerical approaches to quantify information-security risk is scarce. This paper suggests a method to quantify risk in terms of a numeric value or "degree of cybersecurity". To help quantitatively measure the level of cybersecurity for a computer-based information system, we present two indices, the threat-impact index and the cyber-vulnerability index, based on vulnerability trees. By calculating and comparing the indices for various possible security enhancements, managers can select the best security enhancement choice, prioritize the choices by their relative effectiveness, and statistically justify spending resources on the selected choice. By qualifying information security quantitatively, the method can also help managers establish a specific target of security level that they can track.

We illustrate the use of the proposed methodology on the security of supervisory control and data acquisition (SCADA) systems using data from the SCADA system test bed implemented at the University of Louisville as a case study, and then show the use of the proposed indices on this information system before and after two security enhancements." [p. 483]

Keywords: Information security; Risk analysis; Information-security measurement; Security threats; Vulnerability measurement

4.3.1.14 A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System

Title: A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System
Author(s): Maxwell Dondo
Organization: DRDC Ottawa
Publisher: DRDC Ottawa
Publishing Location: Unavailable
Edition: N/A
Pages: 70
Retrieved from: DRDC Ottawa TM 2007-090
Hyperlink: N/A
Date of Publication: May 2007

Abstract:
"In this work, we present a fuzzy systems approach for assessing the relative risk associated with computer network assets. We use this approach to rank vulnerabilities so that analysts can prioritize their work based on the potential risk exposures of assets and networks. We associated vulnerabilities to individual assets, and therefore networks, and develop fuzzy models of the vulnerability attributes. We use fuzzy rules to make an inference on the risk exposure and the likelihood of attack, which allows us to rank the vulnerabilities and show which ones need more immediate attention. We argue that our approach has more meaningful vulnerability prioritisation values than the severity level calculated by the popularly used Common Vulnerability Scoring System (CVSS) approach." [p. i]

4.3.1.15 Cyber Security Vulnerability Assessment of Power Industry

Title: Cyber Security Vulnerability Assessment of Power Industry
Author(s): Yu Jiaxi, Mao Anjia and Guo Zhizhong
Organization: Institute of Electrical and Electronics Engineers (IEEE) Power and Energy Society
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 2200-2205
Retrieved from: Conference Publications, Power Systems Conference and Exposition 2006
Hyperlink:http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04142474
Date of Publication: 2006

Abstract:
"Cyber system plays an important role in supervising and controlling power system. Besides its contribution of much convenience to power industry, the cyber system brings some potential danger because of its inherent vulnerability. It is significant to assess the vulnerability of cyber system, determine its risk to power industry, find out the weak parts, set appropriate strategies to avoid the probable accidents and enhance the safety of the cyber system. After analyzing the threats and vulnerability of cyber system, mainly including the vulnerability of SCADA (Supervisory Control And Data Acquisition) system, EMS (Energy Management System) and MIS (Management Information Systems), this paper proposes two methods, the probabilistic assessment and the integrated risk assessment, to assess the cyber security vulnerability. And some ways are suggested to promote the security of cyber system in power industry." [p. 1]

4.3.1.16 Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems - Part 1: Methodology

Title: Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems - Part 1: Methodology
Author(s): Nian Liu, Jianhua Zhang, Xu Wu
Organization: International Electrotechnical Commission
Publisher: Institute of Electrical and Electronics Engineers (IEEE) Power & Energy Society
Publishing Location: Unavailable
Edition: N/A
Pages: 869-875
Retrieved from: IEEE Transactions on Power Delivery, Vol. 26, No.2
Hyperlink: N/A
Date of Publication: April 2011

Abstract:
"Information security risk assessment of IEC 61850-based power control systems is currently an unsolved problem. One of the reasons is a lack of methodology for asset analysis, which is an important process of risk assessment. As the features of IEC 61850-based power control systems are different from general IT systems, a specific methodology of asset analysis is introduced. Based on the requirements of risk assessment proposed in the BS ISO/IEC 27005 standard, the methodology for asset analysis is separated into asset identification and valuation. For asset identification, a structured asset model is defined to distinguish the assets, and a function-oriented business process model is defined to identify the business process and describe the relations between assets and business processes. For asset valuation, in order to objectively reflect the consequence incurred due to the loss of security properties, three levels of value are defined, which is value of information exchange, asset value of function level, and asset value of system level, respectively. Finally, the implementation procedure of the methodology is described. In the companion paper (Part II), an application instance is presented to support the usefulness of the methodology." [p. 869]

Description:
This paper proposes a "methodology for asset analysis of RA for IEC 61850-based PCSs." [p. 869]

Additional information:
"The content of this paper is organized as follows:
Section II: Concludes the requirements of asset analysis, including identification and valuation of assets, in terms of the BS ISO/IEC 27005.
Section III: Briefly describes the features of IEC 61850-based PCSs which is relevant to the requirements of asset analysis.
Section IV: Presents the outline of the methodology, which includes asset identification, asset valuation, and the overall process.
Sections V and V: The methods for asset identification and asset valuation are introduced, respectively
Section VII: Provides the implementation procedure of the methodology.
Section VIII: Conclusions" [p. 869]

4.3.1.17 Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems - Part II: Application in Substation

Title: Asset Analysis of Risk Assessment for IEC 61850-Based Power Control Systems - Part II: Application in Substation
Author(s): Nian Liu, Jianhua Zhang, Xu Wu
Organization: International Electrotechnical Commission
Publisher: Institute of Electrical and Electronics Engineers (IEEE) Power & Energy Society
Publishing Location: Unavailable
Edition: N/A
Pages: 876-881
Retrieved from: IEEE Transactions on Power Delivery, Vol. 26, No. 2
Hyperlink: N/A
Date of Publication: April 2011

Abstract:
"The information security risk assessment of IEC 61850-based power control systems is currently an unsolved problem. One of the reasons is a lack of methodology for asset analysis, which is an important process of risk assessment. In the companion paper (Part I), a specific methodology of asset analysis for the IEC 61850-based power control systems is introduced. To explain and verify the proposed methodology, the substation automation systems are selected as a typical application field. Before the case study, a basic principle for value assignment in a specific qualitative scale is proposed as a foundation for asset valuation. Then, an instance system based on IEC 61850 is introduced to apply the methodology. The overall procedures of the asset identification and asset valuation are represented step by step. From the results of the application, the methodology can meet the requirements of risk assessment." [p. 876]

Additional Information:
"The content of this paper is organized as follows.

- Section II provides a basic principle for value assignment in a specific qualitative scale.
- Section III introduces an IEC 61850-based SAS for a case study.
- Sections IV and V represent the procedures of asset identification and asset valuation, respectively.
- Finally, conclusions are given in Section VI." [p. 876]

4.3.1.18 Time-To-Compromise Model for Cyber Risk Reduction Estimation

Title: Time-To-Compromise Model for Cyber Risk Reduction Estimation
Author(s): Miles A. McQueen, Wayne F. Boyer, Mark A. Flynn, George A. Beitel
Organization: Idaho National Library
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 17
Retrieved from: Conference: Quality of Protection Workshop, ESORICS, Milano, Italy
Hyperlink: http://www.inl.gov/technicalpublications/Documents/3303757.pdf
Date of Publication: September 1, 2005

Abstract.
"We propose a new model for estimating the time to compromise a system component that is visible to an attacker**.** The model provides an estimate of the expected value of the time-to-compromise as a function of known and visible vulnerabilities, and attacker skill level. The time-to-compromise random process model is a composite of three sub-processes associated with attacker actions aimed at the exploitation of vulnerabilities. In a case study, the model was used to aid in a risk reduction estimate between a baseline Supervisory Control and Data Acquisition (SCADA) system and the baseline system enhanced through a specific set of control system security remedial actions. For our case study, the total number of system vulnerabilities was reduced by 86% but the dominant attack path was through a component where the number of vulnerabilities was reduced by only 42% and the time-to-compromise of that component was increased by only 13% to 30% depending on attacker skill level." [p. 1]

4.3.1.19 A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property

Title: A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property
Author(s): Eva Andrijcic and Barry Horowitz
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 907-923
Retrieved from: Risk Analysis: An International Journal, Vol. 26, No. 4
Hyperlink: N/A
Date of Publication: August 2006

Abstract:
"The article is based on the premise that, from a macro-economic viewpoint, cyber attacks with long-lasting effects are the most economically significant, and as a result require more attention than attacks with short-lasting effects that have historically been more represented in literature. In particular, the article deals with evaluation of cyber security risks related to one type of attack with long-lasting effects, namely, theft of intellectual property (IP) by foreign perpetrators. An International Consequence Analysis Framework is presented to determine (1) the potential macro-economic consequences of cyber attacks that result in stolen IP from companies in the United States, and (2) the likely sources of such attacks. The framework presented focuses on IP theft that enables foreign companies to make economic gains that would have otherwise benefited the U.S. economy. Initial results are presented." [p. 907]

Key words: Cyber security; foreign industrial espionage; input-output modeling; intellectual property theft; macro-economics

4.3.1.20 Quantitative Risk Reduction Estimation Tool for Control Systems - Suggested Approach and Research Needs

Title: Quantitative Risk Reduction Estimation Tool for Control Systems - Suggested Approach and Research Needs
Author(s): Miles McQueen, Wayne Boyer, Mark Flynn, Sam Alessi
Organization: Idaho National Laboratory
Publisher: Unavailable
Publishing Location: United States
Edition: N/A
Pages: 16
Retrieved from: Conference: International Workshop On Complex Network and Infrastructure Protection in Rome, Italy
Hyperlink: http://www.inl.gov/technicalpublications/Documents/3394954.pdf
Date of Publication: March 1st 2006

Abstract:
"For the past year we have applied a variety of risk assessment technologies to evaluate the risk to critical infrastructure from cyber attacks on control systems. More recently, we identified the need for a stand alone control system risk reduction estimation tool to provide owners and operators of control systems with a more useable, reliable, and credible method for managing the risks from cyber attack. Risk is defined as the probability of a successful attack times the value of the resulting loss, typically measured in lives and dollars. Qualitative and ad hoc techniques for measuring risk do not provide sufficient support for cost benefit analyses associated with cyber security mitigation actions. To address the need for better quantitative risk reduction models we surveyed previous quantitative risk assessment research; evaluated currently available tools; developed new quantitative techniques [17] [18]; implemented a prototype analysis tool to demonstrate how such a tool might be used; used the prototype to test a variety of underlying risk calculational engines (e.g. attack tree, attack graph); and identified technical and research needs. We concluded that significant gaps still exist and difficult research problems remain for quantitatively assessing the risk to control system components and networks, but that a useable quantitative risk reduction estimation tool is not beyond reach." [p. 1]

4.3.1.21 Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System

Title: Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System
Author(s): Miles A. McQueen, Wayne F. Boyer, Mark A. Flynn, George A. Beitel
Organization: Idaho National Laboratory
Publisher: Institute of Electrical and Electronics Engineers (IEEE)
Publishing Location: Unavailable
Edition: N/A
Pages: 11
Retrieved from: Proceedings of the 39th Hawaii International Conference on System Sciences
Hyperlink: http://www.if.uidaho.edu/~boyewf/docs/HICSS_paper_Jan_5_2006.pdf
Date of Publication: 2006

Abstract:
"We propose a new methodology for obtaining a quantitative measurement of the risk reduction achieved when a control system is modified with the intent to improve cyber security defense against external attackers**.** The proposed methodology employs a directed graph called a compromise graph, where the nodes represent stages of a potential attack and the edges represent the expected time-to compromise for differing attacker skill levels. Time-to compromise is modeled as a function of known vulnerabilities and attacker skill level. The methodology was used to calculate risk reduction estimates for a specific SCADA system and for a specific set of control system security remedial actions. Despite an 86% reduction in the total number of vulnerabilities, the estimated time-to-compromise was increased only by about 3 to 30% depending on target and attacker skill level." [p. 1]

Additional Information:

- After a brief review of related work, the authors present the proposed methodology by describing and providing the mathematical tools for each of its 10 steps.
- The authors then present the results of a case study, in which the methodology was applied to a small SCADA system (CS60).
- Next, the paper discusses alternative simplistic risk reduction models/metrics, and then concludes with a discussion on future work.

4.3.1.22 Common Methods for Security Risk Analysis

Title: Common Methods for Security Risk Analysis
Author(s): Sylvie Malboeuf, William Sandberg-Maitland, William Dziadyk, Eugen Bacic (Cinnabar Networks Inc.)
Organization: Cinnabar Networks Inc. and DRDC-Ottawa
Publisher: DRDC-Ottawa
Publishing Location: Ottawa, Canada
Edition: Version 1.1
Pages: 78
Retrieved from: DRDC Ottawa Contractor Report (CR) 2004-247
Hyperlink: N/A
Date of Publication: December 2004

Purpose:

- "The purpose of this report is to provide DRDC Scientific Authority with the information necessary to sustain discussions in the NATO Working Group with respect to the status of Canada initiatives and vision on risk management and to contribute to the RTG-21 report [NATO Working Group Report]." [p. 2]

Scope:

- "The scope for this project is to provide a history of Canada' initiatives with respect to risk management and investigate how Canada can augment the Working Group with its experiences and its future initiatives. The report presents conclusions and recommendations for future efforts in this area." [p. 2]

Description:

- "This document contains an overview of Canada's position with respect to risk management. The report covers a survey and research of risk management methodologies and practices applied by Information Technology (IT) managers. A suggestive examination of risk analysis techniques in terms of defining a common framework with a cumulative association to the Common Criteria (CC) is described for forum discussion." [p. 1]

4.3.1.23 Improving Common Security Risk Analysis

Title: Improving Common Security Risk Analysis
Author(s): Task Group IST-049
Organization: NATO - Research and Technology Organization
Publisher: NATO - Research and Technology Organization
Publishing Location: Unavailable
Edition: 1st ed.
Pages: 100
Retrieved from: RTO Technical Report, Final Report of Task Group IST-049: TR-IST-049
Hyperlink: N/A
Date of Publication: September 2008

Description:

- "This report is the final report resulting from the four meetings of the working group called "Improving Common Security Risk Analysis" (IST-049 – RTG-021). The report describes the different methods used by various NATO countries such as EBIOS for France, CRAMM for UK, ITSG-04 for Canada, MAGERIT for Spain. As a first conclusion, the report shows that these methodologies, even if based on similar principles, differ in their knowledge bases (assets, threats, vulnerabilities, …) or type of results (quantitative or qualitative). This makes the risk assessments difficult or impossible to compare when different methods have been used.
- In a second part, the report identifies the main steps which are considered as mandatory for a method to be used by NATO.
- Then the report identifies recommendations which should be taken into account by the existing methods and tools in order to solve the interoperability problem identified in the first part of the document but also to be able to take into account the new NATO concepts such as NNEC. These recommendations mainly concern the integration of dynamic risk analysis and improvement of information exchange. A proposal list of evolution for existing methods and tools concludes this part…
- The final chapter of the report identifies the follow on activities to be conducted within RTO/IST or within other NATO entities." [p.1]

4.3.2 Chemical, Biological, Radioactive, Nuclear, Explosive (CBRNE) Threats

4.3.2.1 Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings

Title: Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings
Author(s): Federal Emergency Management Agency (FEMA)
Organization: Federal Emergency Management Agency (FEMA)
Publisher: Federal Emergency Management Agency (FEMA)
Publishing Location: United States of America
Edition: Unavailable
Pages: 248
Retrieved from: Risk Management Series, FEMA 452
Hyperlink: http://www.fema.gov/library/viewRecord.do?id=1938
Date of Publication: January 2005

Purpose:

- "To provide a clear, flexible and comprehensive methodology to prepare a risk assessment." [p. i]

Objective:

- "Outline methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. Based on those considerations, the methods presented in this How-To-Guide provide a means to assess the risk to the assets and to make risk-based decisions on how to mitigate those risks." [p. i]

Audience:

- "Building sciences community of architects and engineers for private institutions, building owners/operators/managers, and State and local government officials working in the building sciences community." [p. i]

Scope (of the methods):

- "Reducing physical damage to structural and non-structural components of buildings and related infrastructure, and reducing resultant casualties during conventional bomb attacks, as well as chemical, biological and radiological (CBR) agents." [p. i]

Description:

- "This document is written as a How-To Guide. It presents five steps and multiple tasks within each step that will lead you through a process for conducting a risk assessment and selecting mitigation options. It discusses what information is required to conduct a risk assessment, how and where to obtain it, and how to use it to calculate a risk score against each selected threat." [p. i]

4.3.3 Multi-Threat

**Note: The references below present methodologies and tools for assessing or modelling terrorism risk and vulnerability. However, additional references can be found in Section 5.9, "Risk Assessment for Terrorism" under Academic Discussions. The references in Section 5.9 discuss the challenges and limitations in existing methodologies for assessing terrorism risk, while some even propose recommendations or alternative methods.*

4.3.3.1 A Methodology for Modeling Regional Terrorism Risk

Title: A Methodology for Modeling Regional Terrorism Risk
Author(s): Samrat Chatterjee and Mark D. Abkowitz
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1133-1140
Retrieved from: Risk Analysis, Vol. 31, No. 7
Hyperlink: N/A
Date of Publication: July 2011

Abstract:
"Over the past decade, terrorism risk has become a prominent consideration in protecting the well-being of individuals and organizations. More recently, there has been interest in not only quantifying terrorism risk, but also placing it in the context of an all-hazards environment in which consideration is given to accidents and natural hazards, as well as intentional acts. This article discusses the development of a regional terrorism risk assessment model designed for this purpose. The approach taken is to model terrorism risk as a dependent variable, expressed in expected annual monetary terms, as a function of attributes of population concentration and critical infrastructure. This allows for an assessment of regional terrorism risk in and of itself, as well as in relation to man-made accident and natural hazard risks, so that mitigation resources can be allocated in an effective manner. The adopted methodology incorporates elements of two terrorism risk modeling approaches (event-based models and risk indicators), producing results that can be utilized at various jurisdictional levels. The validity, strengths, and limitations of the model are discussed in the context of a case study application within the United States." [p. 1133]

Key words: Critical infrastructure; economic analysis; risk assessment; security; terrorism

Additional Information:
This paper includes sections on:

- Terrorism Risk Assessment approach: risk-cost approach
- Modelling Approach
- Model Estimation
- Model Application: three counties in the state of Tennessee

4.3.3.2 Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection

Title: Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection
Author(s): Henry H. Willis, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, Samuel Neil
Organization: RAND Center for Terrorism Risk Management Policy, prepared for the Department of Homeland Security
Publisher: RAND Corporation
Publishing Location: Saint Monica, CA; Arlington, VA; Pittsburgh, PA
Edition: N/A
Pages: 95
Retrieved from: Rand Corporation Technical Series
Hyperlink: N/A
Date of Publication: 2007

Description:

- The Department of Homeland Security is moving increasingly towards risk analysis and risk-based resource allocation. As a result, the Office of Intelligence and Analysis (OI&A) is exploring how existing risk-analysis tools might be useful for its Homeland Infrastructure Threat and Risk Analysis Center. One of these existing risk analysis tools is the Probabilistic Terrorism Model developed by Risk Management Solutions, Inc. (RMS).
- This report applies the RMS Probabilistic Terrorism Model to compare terrorism risks across different urban areas, to assess terrorism risks within a metropolitan area, and to target intelligence analysis.
- This report presents the results of three applications of the RMS Probabilistic Terrorism Model. These applications produced informative and useful findings, and serve as an example of how insurance-industry models can be used by DHS.

Additional Information:
This document includes sections on:

- Terrorism Risk Models for the Insurance Industry: A New Resource for Intelligence Analysts
- Terrorism Risk Modeling for the Insurance Industry: The RMS Probabilistic Terrorism Model
    - Modeling Terrorist Threats as Probability of Attack
    - Modeling Attack Consequences
- The 3 Applications
- Conclusions and Recommendations for each of the applications

4.3.3.3 Transport Canada Strategic Security Risk Assessment Methodology and User Guide

Title: Transport Canada Strategic Security Risk Assessment Methodology and User Guide
Author(s): Transport Canada
Organization: Transport Canada
Publisher: Transport Canada
Publishing Location: Canada
Edition: Version 6.0
Pages: 21
Retrieved from: Unavailable
Hyperlink: N/A
Date of Publication: March 17, 2006

Objective:

- "Transport Canada's mission is "to ensure that Canadians have a reliable, safe and sustainable transportation system that contributes to Canada's economic growth and social development, and is environmentally friendly."
- The objective of the *Strategic Security Risk Assessment Methodology* is to assess the impact of events and associated risks on Transport Canada's objectives. Events and associated risks are assessed from two perspectives: likelihood of occurrence and impact." [p. 3]

Description:
This document provides step-by-step guidance through each of the 6 steps of the Strategic Security Risk Assessment Methodology. They are:

1. Event identification
2. Threat Assessment
3. Vulnerability Assessment
4. Impact Assessment
5. Risk Assessment
6. (Preliminary) Identification of Actions to Prevent and/or Mitigate Unacceptable Risk

Additional Information:
The users are also provided with supplementary material to support the risk assessment process. They are:

- Guiding principles of the methodology
- Glossary of key terms
- Illustration of the risk assessment methodology
- Risk assessment worksheet
- Criteria for rating threats, vulnerability and impact
- Table for vulnerability assessment

4.3.3.4 Security Risk Assessment Methodology for Communities (RAM-C)

Title: Security Risk Assessment Methodology for Communities (RAM-C)
Author(s): Cal Jaeger, Security Systems and Technology Center, Sandia National Laboratories
Organization: Sandia National Laboratories
Publisher: Sandia National Laboratories
Publishing Location: Albuquerque, New Mexico
Edition: Unavailable
Pages: 106-110
Retrieved from: Conference Publications, from the 38th Annual 2004 International Carnahan Conference on Security Technology
Hyperlink: N/A
Date of Publication: 2004

Abstract
"Sandia National Laboratories (SNL) has developed a number of security risk assessment methodologies (RAMs) for various infrastructures including dams, water systems, electrical transmission, chemical facilities and communities. All of these RAMs consider potential malevolent attacks from different threats, possible undesired events and consequences and determine potential adversary success. They focus on the assessment of these infrastructures to help identify security weaknesses and develop measures to help mitigate the consequences from possible adversary attacks. This paper will focus on RAM-C, the security risk assessment methodology for communities. There are many reasons for a community to conduct a security risk assessment. They include: providing a way to identify vulnerabilities, helping a community to be better prepared in the event of an adversary attack, providing justification for resources to address identified vulnerabilities and planning for future projects. The RAM-C process is a systematic, risk-based approach to assess vulnerabilities and make decisions based on risk. It has provided valuable information to community planners in making security risk decisions." [p. 106]

Additional Information:

- This document provides an overview and description of the RAM-C process, but does not provide prescriptive guidance or detailed material.
- Although RAM-C material is unclassified, distribution is controlled through licensing agreements. Thus, RAM-C is only available to licensed users who attend the accompanying training classes.

4.3.3.5 Roadmap for Modeling Risks of Terrorism to the Homeland

Title: Roadmap for Modeling Risks of Terrorism to the Homeland
Author(s): Yacov Y. Haimes, Lawrence R. Quarles
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 35-41
Retrieved from: Journal of Infrastructure Systems, Vol. 8, No. 2
Hyperlink: N/A
Date of Publication: June 2002

Abstract:
"The terrorist acts of September 11, 2001, were a wake-up call for changing our past practices in ensuring homeland security. The positive results of these changes, however, are accompanied by myriad visible and invisible risks. Accepting change implies assessing and managing these risks in a comprehensive and systemic fashion, avoiding an ad hoc approach. This paper offers a holistic risk assessment and management framework for modeling the risks of terrorism to the homeland. Two major interconnected systems are addressed: the homeland system and the terrorist networks system. In modeling the two systems, the centrality of state variables is highlighted. It is worth noting that the community of risk analysts has been developing and applying systems-based methodologies and tools for many years. The roadmap presented in this paper builds on the findings of many prior analyses." [p. 35]

Additional Information:
This paper includes discussions on:

- Global geo-political dimension: the environment in which the homeland system and terrorist network system operate
- Holistic risk assessment and management process: "a synthesis and amalgamation of the empirical and the normative, the quantitative and the qualitative, and of objective and subjective evidence." [p. 39]
- Modelling infrastructure interdependencies: the emergence of increasingly interdependent infrastructures, and how modeling these interdependencies increases the capacity to assess and manage terrorism risk
- Value of normative-qualitative analyses as a supplement to quantitative analyses

4.3.3.6 Vulnerability Self Assessment Tool (VSAT)

Title: Vulnerability Self Assessment Tool (VSAT)
Author(s): National Counter Terrorism Security Office
Organization: National Counter Terrorism Security Office
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: N/A
Retrieved from: National Counter Terrorism Security Office website
Hyperlink: https://vsat.nactso.gov.uk/OurServices/VSAT.aspx
Date of Publication: Unavailable

Description:

- This webpage provides an overview of the Vulnerability Self Assessment Tool (VSAT). In order to access the VSAT itself, one must contact their local CTSA (Counter Terrorism Security Advisors).

4.4 Miscellaneous

4.4.1 A Classification Scheme for Risk Assessment Methods

Title: A Classification Scheme for Risk Assessment Methods
Author(s): Phillip L. Campbell, Jason E. Stamp
Organization: Sandia National Laboratories, for the United States Department of Energy
Publisher: Unavailable
Publishing Location: United States of America
Edition: N/A
Pages: 29
Retrieved from: Sandia National Laboratories website
Hyperlink: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2004_4233.pdf
Date of Publication: August 2004

Abstract:
"This report presents a classification scheme for risk assessment methods. This scheme, like all classification schemes, provides meaning by imposing a structure that identifies relationships. Our scheme is based on two orthogonal aspects—level of detail, and approach. The resulting structure is shown in Table 1 and is explained in the body of the report.

Table 1 Classification Matrix (Shown also as Table 2 on page 13)

Level		Approach		
		Temporal	Functional	Comparative
Abstract	Expert	① Engagement	④ Sequence	⑦ Principles
Mid-Level	Collaborative	② Exercise	⑤ Assistant	⑧ Best Practice
Concrete	Owner	③ Compliance Testing	⑥ Matrix	⑨ Audit

Each cell in the Table represents a different arrangement of strengths and weaknesses. Those arrangements shift gradually as one moves through the table, each cell optimal for a particular situation. The intention of this report is to enable informed use of the methods so that a method chosen is optimal for a situation given." [p. 3]

Additional information:
“For each of the nine cells in the matrix we identify the method type by name and example.
The matrix helps the user understand
1. what to expect from a given method,
2. how it relates to other methods, and
3. how best to use it” [p. 7]

5 Academic Discussions

Overview

This section includes references which cover a variety of unique topics in relation to risk assessment.

- **Section 5.1**: references that attempt to define risk.
- **Section 5.2**: references that discuss uncertainty in risk assessment.
- **Section 5.3**: references that discuss the use of expert elicitation and judgement in risk assessment.
- **Section 5.4**: references that discuss the value of a life in risk assessment calculations.
- **Section 5.5**: references that discuss the differences between the use of probability and frequency in risk assessment.
- **Section 5.6**: references that discuss the concept of risk acceptability.
- **Section 5.7**: references that discuss the limitations of existing risk assessment methodologies. *Note:* These references are limited to discussions on the technical or mathematical formulations involved in risk assessment. More general reviews on risk assessment or risk management practices are found in Section 5.8.
- **Section 5.8**: references that discuss the evolution of risk, review risk assessment practices, and provide future directions and recommendations.
- **Section 5.9**: references that discuss the challenges and limitations of the application of existing risk assessment methods to terrorism threats.
- **Section 5.10**: miscellaneous references which discuss various approaches to risk assessment.

5.1 Defining Risk

5.1.1 On the Quantitative Definition of Risk

Title: On the Quantitative Definition of Risk
Author(s): Stanley Kaplan and B. John Garrick
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 11-27
Retrieved from: Risk Analysis, Vol. 1, No. 1
Hyperlink: N/A
Date of Publication: 1981

Abstract:
"A quantitative definition of risk is suggested in terms of the idea of a "set of triplets." The definition is extended to include uncertainty and completeness, and the use of Bayes' theorem is described in this connection. The definition is used to discuss the notions of "relative risk," "relativity of risk," and "acceptability of risk"." [p. 11]

5.1.2 Toward A Concept of Risk for Effective Military Decision-Making

Title: Toward A Concept of Risk for Effective Military Decision-Making
Author(s): David R. Mandel
Organization: DRDC Toronto
Publisher: N/A
Publishing Location: Toronto
Edition: N/A
Pages: 31
Retrieved from: DRDC Toronto TR 2007-124 (Technical Report)
Hyperlink: N/A
Date of Publication: December 2007

Abstract:
"This report critically examines existing concepts of risk and offers recommendations for improving the definition of risk and other risk-related terms. The author highlights the fact that the concept of risk is problematic because it is ambiguous and vague. In the vernacular, risk has multiple meanings including (a) risk as potential loss, (b) risk as a probability of a negative event occurring, and (c) risk as variability, volatility, or uncertainty regarding events in the future. In addition, many organisational definitions of risk define the concept in terms of an integration of the probability of a threat and the severity of its potential consequences. The author examines the definition of risk promulgated by (a) the Government of Canada through the Treasury Board Secretariat in its 2001 Integrated Risk Management Framework, (b) the Department of National Defence and Canadian Forces (DND/CF) through the 2002 Joint Doctrine on Risk Management for CF Operations and the 2005 Integrated Risk Management Guideline and Policy documents, and (c) the Canadian Standards Association (CSA) and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). The report concludes with recommendations for the definition of risk, expected utility, and uncertainty, which the author proposes form a set of concepts that can contribute to effective decision making in defence and security contexts." [p. i]

5.2 Uncertainty

5.2.1 Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?

Title: Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1530-1533
Retrieved from: Risk Analysis, Vol. 31, No. 10
Hyperlink: N/A
Date of Publication: October 2011

Abstract:
"Professor Aven has recently noted the importance of clarifying the meaning of terms such as "scientific uncertainty" for use in risk management and policy decisions, such as when to trigger application of the precautionary principle. This comment examines some fundamental conceptual challenges for efforts to define "accurate" models and "small" input uncertainties by showing that increasing uncertainty in model inputs may reduce uncertainty in model outputs; that even correct models with "small" input uncertainties need not yield accurate or useful predictions for quantities of interest in risk management (such as the duration of an epidemic); and that accurate predictive models need not be accurate causal models." [p. 1530]

5.2.2 Fault and Event Tree Analyses for Process Systems Risk Analysis: Uncertainty Handling Formulations

Title: Fault and Event Tree Analyses for Process Systems Risk Analysis: Uncertainty Handling Formulations
Author(s): Refaul Ferdous, Faisal Khan, Rehan Sadiq, Paul Amyotte, and Brian Veitch
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 86- 107
Retrieved from: Risk Analysis, Vol. 31, No. 1
Hyperlink: N/A
Date of Publication: January 2011

Abstract:
"Quantitative risk analysis (QRA) is a systematic approach for evaluating likelihood, consequences, and risk of adverse events. QRA based on event (ETA) and fault tree analyses (FTA) employs two basic assumptions. The first assumption is related to likelihood values of input events, and the second assumption is regarding interdependence among the events (for ETA) or basic events (for FTA). Traditionally, FTA and ETA both use crisp probabilities; however, to deal with uncertainties, the probability distributions of input event likelihoods are assumed. These probability distributions are often hard to come by and even if available, they are subject to incompleteness (partial ignorance) and imprecision. Furthermore, both FTA and ETA assume that events (or basic events) are independent. In practice, these two assumptions are often unrealistic. This article focuses on handling uncertainty in a QRA framework of a process system. Fuzzy set theory and evidence theory are used to describe the uncertainties in the input event likelihoods. A method based on a dependency coefficient is used to express interdependencies of events (or basic events) in ETA and FTA. To demonstrate the approach, two case studies are discussed." [p. 86]

5.2.3 Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making

Title: Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making
Author(s): Terje Aven, Enrico Zio
Organization: N/A
Publisher: Elsevier
Publishing Location: Unavailable
Edition: N/A
Pages: 64-74
Retrieved from: Reliability Engineering and System Safety, Vol. 96, No. 2
Hyperlink: N/A
Date of Publication: January 2011

Abstract
"This paper discusses the challenges involved in the representation and treatment of uncertainties in risk assessment, taking the point of view of its use in support to decision making. Two main issues are addressed: (1) how to faithfully represent and express the knowledge available to best support the decision making and (2) how to best inform the decision maker. A general risk-uncertainty framework is presented which provides definitions and interpretations of the key concepts introduced. The framework covers probability theory as well as alternative representations of uncertainty, including interval probability, possibility and evidence theory." [p. 64]

5.2.4 Imprecise Reliability

Title: Imprecise Reliability
Author(s): Frank P.A. Coolen, Lev V. Utkin
Organization: N/A
Publisher: Wiley
Publishing Location: Unavailable
Edition: Unavailable
Pages: 6
Retrieved from: Encyclopedia of Quantitative Risk Analysis and Assessment
Hyperlink: http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0476/pdf
Date of Publication: 2008

Abstract:
"We present a concise overview of imprecise reliability, particularly focusing on reliability theory with uncertainty quantified via lower and upper probabilities. We discuss the main approaches and opportunities of the theory, include references to guide further study, and briefly discuss some research challenges.[22]"

Keywords: expert judgments; imprecise Dirichlet model; lower and upper probability; natural extension; nonparametric predictive inference; robustness

[22] From http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0476/abstract

5.2.5 Assessment and Communication of Risks to National Security: Understanding Human Capabilities and Limitations

Title: Assessment and Communication of Risks to National Security: Understanding Human Capabilities and Limitations
Author(s): Dr. David R. Mandel
Organization: Adversarial Intention Section, DRDC Toronto
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 34 (slides)
Retrieved from: Presentation for Defence Security Innovation 2007, Quebec, Quebec
Hyperlink: N/A
Date of Publication: November 15, 2007

Description:

- This presentation discusses risk with respect to the uncertainties that arise from human capabilities and limitations.

Additional Information:
This presentation discusses the following topics:

- Concepts and definitions of risk
- Factors that influence risk assessment
- Communication of uncertainty, including recommendations

5.2.6 Risk Management and Precaution: Insights on the Cautious Use of Evidence

Title: Risk Management and Precaution: Insights on the Cautious Use of Evidence
Author(s): Steve E. Hrudey and William Leiss
Organization: N/A
Publisher: National Institute of Environmental Health Sciences
Publishing Location: Unavailable
Edition: N/A
Pages: 1577-1581
Retrieved from: Environmental Health Perspectives, Vol. 111, No. 13
Hyperlink: N/A
Date of Publication: October 2003

Abstract
"Risk management, done well, should be inherently precautionary. Adopting an appropriate degree of precaution with respect to feared health and environmental hazards is fundamental to risk management. The real problem is in deciding how precautionary to be in the face of inevitable uncertainties, demanding that we understand the equally inevitable false positives and false negatives from screening evidence. We consider a framework for detection and judgment of evidence of well-characterized hazards, using the concepts of sensitivity, specificity, positive predictive value, and negative predictive value that are well established for medical diagnosis. Our confidence in predicting the likelihood of a true danger inevitably will be poor for rare hazards because of the predominance of false positives; failing to detect a true danger is less likely because false negatives must be rarer than the danger itself. Because most controversial environmental hazards arise infrequently, this truth poses a dilemma for risk management.

Key words: complacency, false negatives, false positives, futility, positive predictive value, zero risk." [p. 1577]

Additional Information:
This paper includes discussions on:

- Interpreting evidence about hazards
- Roots of complacency
- Exercising caution and the precautionary principle
- Caution vs. Futility

5.2.7 Internal Dose, Uncertainty Analysis and Complexity of Risk Models

Title: Internal Dose, Uncertainty Analysis and Complexity of Risk Models
Author(s): Louis Anthony Cox Jr.
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 841-852
Retrieved from: Environment International, Vol. 25, No. 6-7
Hyperlink: N/A
Date of Publication: September 1999

Abstract:
"Practitioners and consumers of risk assessments often wonder whether the trend toward more complex risk models, incorporating increasing amounts of biological knowledge and increasing numbers of biologically interpretable parameters, actually leads to better risk estimates. A contrary view might be that the need to estimate more uncertain quantities undermines the advantages of greater descriptive realism so much that the final risk estimates are less certain than the ones traditionally obtained from simpler, less realistic, statistical curve-fitting models. In opposition to this pessimistic view is the widespread common-sense notion that including more information in a risk model can never worsen (and will usually improve) the resulting risk estimates. This paper appeals to mathematical arguments to resolve these conflicting intuitions. First, it emphasizes the fact that risk depends on multiple inputs only through a small number of reduced quantities - perhaps on only one, which would then be defined as internal dose. Thus, uncertainty about risk may have limited sensitivity to uncertainties in the original input quantities. The concept of internal dose and its possible algebraic relations to the original input quantities are clarified using concepts from dimensional analysis. Then, the question of whether greater model complexity leads to better or worse risk estimates is addressed in an information-theoretic framework, using entropies of probability distributions to quantify uncertainties. Within this framework, it is shown that models with greater intrinsic or structural complexity (meaning complexity that cannot be eliminated by reformulating the model in terms of its reduced quantities) lead to better-informed, and hence more certain (lower-entropy) risk estimates. The compatibility of this result with results from decision theory, in which expected loss rather than entropy is used as a criterion, is discussed.[23]"

[23] From http://www.sciencedirect.com/science/article/pii/S0160412099000628

5.2.8 Uncertainties in Risk Analysis: Six Levels of Treatment

Title: Uncertainties in Risk Analysis: Six Levels of Treatment
Author(s): M. Elisabeth Paté-Cornell
Organization: N/A
Publisher: Elsevier Science Limited
Publishing Location: Northern Ireland
Edition: N/A
Pages: 95-111
Retrieved from: Reliability Engineering and System Safety, vol. 54, issues 2-3
Hyperlink: N/A
Date of Publication: 1996

Abstract:
"This paper examines different levels of analytical sophistication in the treatment of uncertainties in risk analysis, and the possibility of transfer of experience across fields of application. First, this paper describes deterministic and probabilistic methods of treatment of risk and uncertainties, and the different viewpoints that shape these analyses. Second, six different levels of treatment of uncertainty are presented and discussed in the light of the evolution of the risk management philosophy in the U.S. Because an in-depth treatment of uncertainties can be complex and costly, this paper then discusses when and why a full (two-tier) uncertainty analysis is justified. In the treatment of epistemic uncertainty, an unavoidable and difficult problem is the encoding of probability distributions based on scientific evidence and expert judgments. The last sections include a description of different approaches to the aggregation of expert opinions and their use in risk analysis, and a recent example of methodology and application (in seismic hazard analysis) that can be transferred to other domains." [p. 95]

5.3 Expert Elicitation and Judgement

5.3.1 Combining the Opinions of Experts Who Partition Events Differently

Title: Combining the Opinions of Experts Who Partition Events Differently
Author(s): Robert F. Bordley
Organization: General Motors Research Laboratories and University of Michigan
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 38-46
Retrieved from: Decision Analysis, Vol. 6, No. 1
Hyperlink: N/A
Date of Publication: March 2009

Abstract:
"This paper focuses on updating a client's beliefs about an event based on information about the different probabilities that various experts assess for that event. A substantial literature solves this problem when all experts assess their probabilities over the same partitioning of the possible outcomes of an event. But different experts often think about the same problem in quite different ways. This can lead to differences in how experts prefer to partition the possible outcomes of an event. Forcing the experts to use a common partition could lead to less informative probability assessments. Thus, this paper presents a new approach for combining probability assessments from different experts, which allows experts to assess their probability assessments across different partitionings." [p. 38]

Key words: probability elicitation; decision analysis; forecasts: combining; probability: group; incoherence

5.3.2 Aggregating Probabilistic Forecasts from Incoherent and Abstaining Experts

Title: Aggregating Probabilistic Forecasts from Incoherent and Abstaining Experts
Author(s): Joel B. Predd, Daniel N. Osherson, Sanjeev R. Kulkarni, H. Vincent Poor
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 177-189
Retrieved from: Decision Analysis, Vol. 5, No. 4
Hyperlink: N/A
Date of Publication: December 2008

Abstract:
"Decision makers often rely on expert opinion when making forecasts under uncertainty. In doing so, they confront two methodological challenges: the elicitation problem, which requires them to extract meaningful information from experts; and the aggregation problem, which requires them to combine expert opinion by resolving disagreements. Linear averaging is a justifiably popular method for addressing aggregation, but its robust simplicity makes two requirements on elicitation. First, each expert must offer probabilistically coherent forecasts; second, each expert must respond to all our queries. In practice, human judges (even experts) may be incoherent, and may prefer to assess only the subset of events about which they are comfortable offering an opinion. In this paper, a new methodology is developed for combining expert assessment of chance. The method retains the conceptual and computational simplicity of linear averaging, but generalizes the standard approach by relaxing the requirements on expert elicitation. The method also enjoys provable performance guarantees, and in experiments with real-world forecasting data is shown to offer both computational efficiency and competitive forecasting gains as compared to rival aggregation methods. This paper is relevant to the practice of decision analysis, for it enables an elicitation methodology in which judges have freedom to choose the events they assess." [p. 177]

5.3.3 Getting the Right Mix of Experts

Title: Getting the Right Mix of Experts
Author(s): Jason R.W. Merrick
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 43-52
Retrieved from: Decision Analysis, Vol. 5, No. 1
Hyperlink: N/A
Date of Publication: March 2008

Abstract:
"The Bayesian approach to combining expert opinions is well developed, providing a decision maker's posterior beliefs after receiving advice from people with deep knowledge in a given subject. A necessary part of these models is the inclusion of dependencies between the experts' judgments, often justified by an overlap in the information on which the experts base their judgments. In this paper, we propose a hierarchical structure different than those previously proposed, where the mixing distribution is treated nonparametrically with a Dirichlet process. This makes our overall model a Dirichlet process mixture and allows for experts' model parameters to be equal in the mixture. We apply this approach to published expert judgment data, demonstrating that the decision maker's posterior distributions on the quantities of interest are not restricted to specific parametric forms, even allowing for multiple modes, and are thus more intuitively appealing." [p. 43]

Key words: decision analysis; inference; expert judgment aggregation; forecasting; combining statistics; Bayesian; nonparametric; Dirichlet process mixtures

5.3.4 Expert Elicitation for Risk Assessment

Title: Expert Elicitation for Risk Assessment
Author(s): Wiedlea, A. C. K.
Organization: N/A
Publisher: Wiley
Publishing Location: Unavailable
Edition: Unavailable
Pages: 7
Retrieved from: Encyclopedia of Quantitative Risk Analysis and Assessment
Hyperlink: http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0490/pdf
Date of Publication: 2008

Abstract:
"Expert elicitation—the use of structured, calibrated questions to gather qualitative risk information—is a key risk assessment tool. Particularly when there does not exist sufficient observed data to estimate the nature of a risk process, or in cases when a system risk is generated by the interactions of a complex set of component interactions, qualitative information gathered from subject matter experts may be the best, if not the only, source of relevant information. Ensuring that information gathered from subject matter experts is relatively free from bias and probability logic inconsistency is a key interest of elicitation research.[24]"

Keywords: expert elicitation; risk estimation; subject matter expert opinion; expert knowledge; uncertainty; risk management

Description:
- This paper offers "an attempt to distil from the literature, a set of models for different risk expert elicitation scenarios, along with an introduction to the various uses of risk elicitation that have been reported in the literature." [p. 1]

Additional Information:
- The author distinguishes four different categories of risk origination. They are: basic events, system processes, competitive games, and social negotiation.

[24]From http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0490/abstract

5.3.5 Expert Judgement in Risk Assessment

Title: Expert Judgement in Risk Assessment
Author(s): Kelvin Leung, Simona Verga
Organization: Centre for Security Science, Operations Research Team
Publisher: Defence R&D Canada - CORA
Publishing Location: Canada
Edition: N/A
Pages: 58
Retrieved from: DRDC CORA TM 2007-57
Hyperlink: N/A
Date of Publication: December 2007

Abstract:
"Decision and risk analysis models often require both qualitative and quantitative assessments of uncertain events; in many cases, expert knowledge is essentially the only source of good information. Over the last decade, uncertainty analysis has become an increasingly important part of operations research models. The growing use of risk assessment in government and corporate planning and operations has also increased the role of expert judgement in providing information for decision making.

Elicitation of experts' opinions is frequently used to support decision making in many different areas, from forecasting in the financial world to assessing the risk of terrorist attacks in the national security domain. The use of expert judgements has provoked questions related to the practice of utilizing experts' opinions and to the accuracy of the obtained results. This work reviews some approaches for eliciting and aggregating expert judgements as inputs into the risk assessment process, and looks at methods of assessing the degree of confidence associated with these subjective inputs, as well as confidence in the overall process.

The research synthesized in this report outlines the elicitation process and highlights both its statistical and psychological perspectives. It looks at ways to evaluate the accuracy of elicitation; it presents techniques for the aggregation of probability distributions from multiple experts; and it summarizes a conceptual framework for the quality verification of risk assessment. Two examples of the application of formal elicitation in the nuclear industry and a business study are also discussed in the Appendix." [p. i]

5.3.6 Elicitation from Large, Heterogeneous Expert Panels: Using Multiple Uncertainty Measures to Characterize Information Quality for Decision Analysis

Title: Elicitation from Large, Heterogeneous Expert Panels: Using Multiple Uncertainty Measures to Characterize Information Quality for Decision Analysis
Author(s): Sandra Hoffmann, Paul Fischbeck, Alan Krupnick, Michael McWilliams
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 91-109
Retrieved from: Decision Analysis, Vol. 4, No. 2
Hyperlink: N/A
Date of Publication: June 2007

Abstract:
"Decision analysts are frequently called on to help inform decision makers in cases involving considerable uncertainty. In such situations, expert elicitation of parameter values is frequently used to supplement more conventional research. Expert elicitations typically rely on small panels of experts. However, in cases where the information needed for risk management must draw on a broad range of disciplines or types of professional backgrounds and experience, a larger, more heterogeneous expert panel is needed. In this paper we develop a formal protocol and a suite of uncertainty measures for this work. The protocol uses formal survey methods to take advantage of variation in individual expert uncertainty and heterogeneity among experts as a means of quantifying and comparing sources of uncertainty about parameters of interest. We illustrate the use of this protocol with an expert elicitation on the distribution of foodborne illness in the United States across foods. In the survey, experts are asked to attribute illnesses associated with one of eleven major foodborne pathogens to the consumption of one of eleven categories of food. Results show how the distributions of multiple measures of uncertainty (e.g., agreement of experts and uncertainty in knowledge), made feasible by use of a large panel of experts, can help identify which of several types of risk management actions may be most appropriate." [p. 91]

Description:
The protocol developed in this study:

- "Makes use of the heterogeneity inherent in large expert panels to create internal validity checks on the quality of information available to decision makers.
- This is accomplished by comparing four measures of uncertainty about estimates of interest: (1) variability in expert judgment; (2) the level of agreement between experts 'assessments and prior estimates based on primary data; (3) individual experts' uncertainty about their own assessments; and (4) variability in individual experts' uncertainty about their own best estimates.
- Use of a large expert panel allows statistical analysis of these uncertainty measures that would not be possible with a small panel. This statistical analysis, in turn, provides a means of characterizing the degree of uncertainty associated with parameter estimates, understanding the nature of that uncertainty, and providing decision makers with a basis for reaching a reasoned judgment about the adequacy of the information and the need for further data development or research." [p. 92]

5.3.7 Analysis of Correlated Expert Judgements from Extended Pairwise Comparisons

Title: Analysis of Correlated Expert Judgements from Extended Pairwise Comparisons
Author(s): Jason R. W. Merrick, J. Rene van Dorp, Amita Singh
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 17-29
Retrieved from: Decision Analysis, Vol. 2, No. 1
Hyperlink: N/A
Date of Publication: March 2005

Abstract:
"We develop a Bayesian multivariate analysis of expert judgment elicited using an extended form of pairwise comparisons. The method can be used to estimate the effect of multiple factors on the probability of an event and can be applied in risk analysis and other decision problems. The model, which parallels Bayesian models for combining expert judgments, provides predictions of the quantity of interest that incorporate dependencies among the various experts. In this form we may learn about the dependencies between the experts from their responses. The analysis is applied to a real data set of expert judgments elicited during the Washington State Ferries Risk Assessment. The effect of the statistical dependence among experts is compared to an analysis assuming independence among them." [p.17]

Key words: expert judgment; pairwise comparisons; Bayesian statistics; multivariate analysis

5.3.8 An Illustrative Canadian Strategic Risk Assessment

Title: An Illustrative Canadian Strategic Risk Assessment
Author(s): James S. Finan and W.D. Macnamara
Organization: National Defence and the Canadian Forces
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 29-34
Retrieved from: Canadian Military Journal, Vol. 2, No. 3
Hyperlink: http://www.journal.forces.gc.ca/vo2/no3/doc/29-34-eng.pdf
Date of Publication: Autumn 2001

Description:

- "In this paper, we have set out to demonstrate the application of one particular method for using 'expert choice' — the Analytic Hierarchy Process (AHP). This illustrates a technique by means of which future-oriented strategic risk assessments may be done systematically, permitting subsequent periodic comparative repetition, and providing an 'audit trail' of the rationale for conclusions." [p. 29]

Additional Information:

- This paper provides an overview of the Analytic Hierarchy Process. It then illustrates the technique by applying it to 25 issues, risks, or threats which are likely to appear in a strategic risk assessment.

5.4 Value of a Life

5.4.1 Value of Human Life Estimates in Homeland Security Risk Analysis

Title: Value of Human Life Estimates in Homeland Security Risk Analysis
Author(s): David Daniels
Organization: N/A
Publisher: N/A
Publishing Location: N/A
Edition: N/A
Pages: 17 (slides)
Retrieved from: Presentation, 3rd Annual SARMA (Security Analysis and Risk Management) Conference, Arlington VA
Hyperlink: N/A
Date of Publication: June 17, 2009

Description:

- This presentation provides a general discussion on the issue of estimating the value of a human life.

Additional Information:
This presentation discusses the following topics:

- Why try to measure the value of human life?
- Value of life methods and the critical questions that ensue
- How to measure the value of life?
    - Legal value of Life
    - Stated preference, revealed preference studies (Willingness to pay and Willingness to accept approaches)
- Value of life in homeland security is essentially a policy decision

5.4.2 The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World

Title: The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World
Author(s): W. Kip Viscusi, Joseph E. Aldy
Organization: Harvard Law School, John M. Olin Center for Law, Economics and Business
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 128
Retrieved from: Harvard Law School John M. Olin Center for Law, Economics and Business Discussion Paper Series, Paper 392
Hyperlink: http://lsr.nellco.org/harvard_olin/392/
Date of Publication: November 2002

Abstract:
"A substantial literature over the past thirty years has evaluated tradeoffs between money and fatality risks. These values in turn serve as estimates of the value of a statistical life. This article reviews more than 60 studies of mortality risk premiums from ten countries and approximately 40 studies that present estimates of injury risk premiums. This critical review examines a variety of econometric issues, the role of unionization in risk premiums, and the effects of age on the value of a statistical life. Our meta-analysis indicates an income elasticity of the value of a statistical life from about 0.5 to 0.6. The paper also presents a detailed discussion of policy applications of these values of a statistical life estimates and related issues, including risk-risk analysis." [Introductory pages]

5.5 Probability and Frequency in Risk Assessment

5.5.1 Some Limitations of Frequency as a Component of Risk: An Expository Note

Title: Some Limitations of Frequency as a Component of Risk: An Expository Note
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 171-175
Retrieved from: Risk Analysis, Vol. 29, No. 2
Hyperlink: N/A
Date of Publication: February 2009

Abstract:
"Students of risk analysis are often taught that “risk is frequency times consequence” or, more generally, that risk is determined by the frequency *and* severity of adverse consequences. But is it? This expository note reviews the concepts of frequency as average annual occurrence rate and as the reciprocal of mean time to failure (MTTF) or mean time between failures (MTBF) in a renewal process. It points out that if two risks (represented as two (*frequency*, *severity*) pairs for adverse consequences) have identical values for *severity* but different values of *frequency*, then it is not necessarily true that the one with the smaller value of *frequency* is preferable—and this is true no matter how *frequency* is defined. In general, there is not necessarily an increasing relation between the reciprocal of the mean time until an event occurs, its long-run average occurrences per year, and other criteria, such as the probability or expected number of times that it will happen over a specific interval of interest, such as the design life of a system. Risk depends on more than frequency and severity of consequences. It also depends on other information about the probability distribution for the time of a risk event that can become lost in simple measures of event “frequency.” More flexible descriptions of risky processes, such as point process models can avoid these limitations." [p. 171]

5.5.2 Differences between Probability and Frequency Judgments: The Role of Individual Differences in Working Memory Capacity

Title: Differences between Probability and Frequency Judgments: The Role of Individual Differences in Working Memory Capacity
Author(s): Amber Sprenger, Michael R. Dougherty
Organization: Department of Psychology, University of Maryland
Publisher: Elsevier
Publishing Location: Unavailable
Edition: N/A
Pages: 202-211
Retrieved from: Organizational Behavior and Human Decision Processes, Vol. 99, No. 2
Hyperlink: N/A
Date of Publication: March 2006

Abstract:
"Most theories of probability judgment assume that judgments are made by comparing the strength of a focal hypothesis relative to the strength of alternative hypotheses. In contrast, research suggests that frequency judgments are assessed using a non-comparative process; the strength of the focal hypothesis is assessed without comparing it to the strength of alternative hypotheses. We tested this distinction between probability and frequency judgments using the alternative outcomes paradigm (Windschitl, Young, & Jenson, 2002). Assuming that judgments of probability (but not judgments of frequency) entail comparing the focal hypothesis with alternative hypotheses, we hypothesized that probability judgments would be sensitive to the distribution of the alternative hypotheses and would be negatively correlated with individual differences in working memory (WM) capacity. In contrast, frequency judgments should be unrelated to the distribution of the alternatives and uncorrelated with WM-capacity. Results supported the hypotheses." [p. 202]

Purpose and Results:
1. Explore the cognitive processes involved in making judgements on probability versus frequency:
    - "Argued that only probability judgments entailed the use of a comparison process to derive the judgment. Several aspects of our results were consistent with this hypothesis." [p. 210]
2. Examine the accuracy of judgements for frequency and probability:
    - "Although we found differences in absolute accuracy between frequency and probability judgments, there were no differences in relative accuracy between the two judgment conditions. This is an important finding because it suggests that conclusions that frequency judgments are more accurate than probability judgments may well be limited to one definition of accuracy, absolute accuracy." [p. 210]

5.5.3 Frequency versus Probability Formats in Statistical Word Problems

Title: Frequency versus Probability Formats in Statistical Word Problems
Author(s): Jonathan St. B.T. Evans, Simon J. Handley, Nick Perham, David E. Over, Valerie A. Thompson
Organization: N/A
Publisher: Elsevier ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 197-213
Retrieved from: Cognition, Vol. 77
Hyperlink: N/A
Date of Publication: December 2000

Abstract
"Three experiments examined people's ability to incorporate base rate information when judging posterior probabilities. Specifically, we tested the...conclusion[25] that people's reasoning appears to follow Bayesian principles when they are presented with information in a frequency format, but not when information is presented as one case probabilities. First, we found that frequency formats were not generally associated with better performance than probability formats unless they were presented in a manner which facilitated construction of a set inclusion mental model. Second, we demonstrated that the use of frequency information may promote biases in the weighting of information. When participants are asked to express their judgements in frequency rather than probability format, they were more likely to produce the base rate as their answer, ignoring diagnostic evidence." [p. 197]

[25] From following reference: Cosmides, L., &Tooby, J. (1996). Are humans good intuitive statisticians after all? Rethinking some conclusions from the literature on judgement under uncertainty. Cognition, 58, 1–73.

5.5.4 Violence Risk Assessment and Risk Communication: The Effects of Using Actual Cases, Providing Instruction, and Employing Probability Versus Frequency Formats

Title: Violence Risk Assessment and Risk Communication: The Effects of Using Actual Cases, Providing Instruction, and Employing Probability versus Frequency Formats
Author(s): Paul Slovic, John Monahan, Donald G. MacGregor
Organization: N/A
Publisher: Springer
Publishing Location: Unavailable
Edition: N/A
Pages: 271-296
Retrieved from: Law and Human Behavior, Vol. 24, No. 3
Hyperlink: N/A
Date of Publication: June 2000

Abstract:
"This article describes studies designed to inform policy makers and practitioners about factors influencing the validity of violence risk assessment and risk communication. Forensic psychologists and psychiatrists were shown case summaries of patients hospitalized with mental disorder and were asked to judge the likelihood that the patient would harm someone within six months after discharge from the hospital. They also judged whether the patient posed a high risk, medium risk, or low risk of harming someone after discharge. Studies 1 and 2 replicated, with real case summaries as stimuli, the response-scale effects found by Slovic and Monahan (1995). Providing clinicians with response scales allowing more discriminability among smaller probabilities led patients to be judged as posing lower probabilities of committing harmful acts. This format effect was not eliminated by having clinicians judge relative frequencies rather than probabilities or by providing them with instruction in how to make these types of judgments. In addition, frequency scales led to lower mean likelihood judgments than did probability scales, but, at any given level of likelihood, a patient was judged as posing higher risk if that likelihood was derived from a frequency scale (e.g., 10 out of 100) than if it was derived from a probability scale (e.g., 10%). Similarly, communicating a patient's dangerousness as a relative frequency (e.g., 2 out of 10) led to much higher perceived risk than did communicating a comparable probability (e.g., 20%). The different reactions to probability and frequency formats appear to be attributable to the more frightening images evoked by frequencies. Implications for risk assessment and risk communication are discussed." [p. 271]

5.5.5 Are Humans Good Intuitive Statisticians After All? Rethinking Some Conclusions from the Literature on Judgment under Uncertainty

Title: Are Humans Good Intuitive Statisticians After All? Rethinking Some Conclusions from the Literature on Judgment under Uncertainty
Author(s): Leda Cosmides, John Tooby
Organization: Centre for Evolutionary Psychology, University of California
Publisher: Elsevier ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 1-73
Retrieved from: Cognition, Vol. 58, No. 1
Hyperlink: N/A
Date of Publication: 1996

Abstract
"Professional probabilists have long argued over what probability means, with, for example, Bayesians arguing that probabilities refer to subjective degrees of confidence and frequentists arguing that probabilities refer to the frequencies of events in the world. Recently, Gigerenzer and his colleagues have argued that these same distinctions are made by untutored subjects, and that, for many domains, the human mind represents probabilistic information as frequencies. We analyze several reasons why, from an ecological and evolutionary perspective, certain classes of problem solving mechanisms in the human mind should be expected to represent probabilistic information as frequencies. Then, using a problem famous in the "heuristics and biases" literature for eliciting base rate neglect, we show that correct Bayesian reasoning can be elicited in 76% of subjects- indeed, 92% in the most ecologically valid condition- simply by expressing the problem in frequentist terms. This result adds to the growing body of literature showing that frequentist representations cause various cognitive biases to disappear, including overconfidence, the conjunction fallacy, and base-rate neglect. Taken together, these new findings indicate that the conclusion most common in the literature on judgment under uncertainty- that our inductive reasoning mechanisms do not embody a calculus of probability - will have to be re-examined. From an ecological and evolutionary perspective, humans may turn out to be good intuitive statisticians after all." [p. 1]

5.6 Risk Acceptability

5.6.1 Propositions for Using Risk Acceptance Criteria

Title: Propositions for Using Risk Acceptance Criteria
Author(s): Rudolf B. Jongejan, Sebastiaan N. Jonkman, Terje Aven, Ben J.M. Ale
Organization: N/A
Publisher: Inderscience Enterprises Ltd.
Publishing Location: Switzerland
Edition: N/A
Pages: 79-90
Retrieved from: International Journal of Business Continuity and Risk Management, Vol. 2, No.1
Hyperlink: http://www.inderscience.com/storage/f413926810125711.pdf
Date of Publication: 2011

Abstract:
"Risk acceptance and tolerability criteria are tools that are used to evaluate and control risks. Although such criteria have been used for many years in different sectors of applications, their rationale and use are still being discussed. Three issues commonly addressed are:
1) the type and form of the criteria (e.g., general formulations compared to tailor-made criteria for specific applications);
2) the criteria's relationship with value generation;
3) methods for and uncertainties in the risk assessments that are used to verify that the criteria are met.

In this paper, we take a closer look at these issues. The aim of the paper is to stimulate the ongoing debate about the applications of risk criteria. A number of propositions is presented that are based on three case-studies: the use of acceptance and tolerability criteria in the Dutch flood safety policy, the Dutch major hazards policy, and the Norwegian petroleum industry." [p. 79-80]

5.6.2 The Acceptability and the Tolerability of Societal Risks: A Capabilities-Based Approach

Title: The Acceptability and the Tolerability of Societal Risks: A Capabilities-Based Approach
Author(s): Colleen Murphy, Paolo Gardoni
Organization: N/A
Publisher: Springer
Publishing Location: Unavailable
Edition: N/A
Pages: 77-92
Retrieved from: Science and Engineering Ethics, Vol. 14, Issue 1
Hyperlink:
http://philosophy.tamu.edu/~cmmurphy/Research/acceptable%20risk%20volume%20version.pdf
Date of Publication: March 2008

Abstract:
"In this paper, we present a Capabilities-based Approach to the acceptability and the tolerability of risks posed by natural and man-made hazards. We argue that judgments about the acceptability and/or tolerability of such risks should be based on an evaluation of the likely societal impact of potential hazards, defined in terms of the expected changes in the capabilities of individuals. Capabilities refer to the functionings, or valuable doings and beings, individuals are able to achieve given available personal, material, and social resources. The likely impact of a hazard on individuals' capabilities should, we argue, be compared against two separate thresholds. The first threshold specifies the minimum level of capabilities attainment that is acceptable in principle for individuals to have in the aftermath of a hazard over any period of time. This threshold captures the level that individuals' capabilities ideally should not fall below. A risk is acceptable if the probability that the attained capabilities will be less than the acceptable level is sufficiently small. In practice, it can be tolerable for some individuals to temporarily fall below the acceptable threshold, provided this situation of lower capabilities attainment is temporary, reversible, and the probability that capabilities will fall below a tolerability threshold is sufficiently small. This second, tolerable threshold delimits an absolute minimum level of capabilities attainment below which no individual in a society should ever fall, regardless of whether that level of capabilities attainment is temporary or reversible. In this paper, we describe and justify this Capabilities-based Approach to the acceptability and tolerability of risks. We argue that the proposed theoretical framework avoids the limitations in current approaches to acceptable risk. The proposed approach focuses the attention of risk analysts directly on what should be our primary concern when judging the acceptability and the tolerability of risks, namely, how risks impact the well-being of individuals in a society. Also, our Capabilities-based Approach offers a transparent, easily communicable way for determining the acceptability and the tolerability of risks." [p. 77]

5.7 Critiques and Limitations of Risk Assessment Methods

5.7.1 Improving Risk Matrices: The Advantages of Logarithmically Scaled Axes

Title: Improving Risk Matrices: The Advantages of Logarithmically Scaled Axes
Author(s): E.S. Levine
Organization: Department of Homeland Security, Office of Risk Management and Analysis, Washington DC, USA
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 209-222
Retrieved from: Journal of Risk Research, Vol. 15, No. 2
Hyperlink: N/A
Date of Publication: February 2012

Abstract:
"Risk matrices are a common tool used throughout the public and private sector to assess and manage risk qualitatively. However, these matrices have well-documented shortcomings when used for either assessment or management that can be shown by assuming a quantitative scale for the likelihood and consequence axes. This article describes the construction of a logarithmically scaled risk assessment matrix which alleviates some of the limitations inherent in using linearly structured risk matrices. In particular, logarithmic risk matrices can better differentiate between hazards with a large dynamic range in risks and, when used in combination with a new categorization scheme, the categorization of risks is more straightforward. These properties are demonstrated using a hypothetical example. Finally, the defensibility of logarithmic matrices is examined in the context of previously proposed rules for developing risk matrices." [p. 209]

Purpose:

- "To describe the advantages of logarithmically scaled risk matrices, when used along with a new risk categorization scheme, and demonstrate these matrices' defensibility." [p. 211]

Additional Information:
This paper includes the following sections:

- "In Section 2, we provide background information on how qualitative rankings of likelihood and consequence are combined to produce risk.
- In Section 3, we describe the use of logarithmic scales in likelihood and consequence along with a new risk classification scheme, and
- In Section 4, we describe an example of such a matrix.
- In Section5, we explore the formal justification of a logarithmic risk matrix in the context of previously described rules for their design." [p. 211]

5.7.2 Problems with Scoring Methods and Ordinal Scales in Risk Assessment

Title: Problems with Scoring Methods and Ordinal Scales in Risk Assessment
Author(s): D. Hubbard, D. Evans
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 1-10
Retrieved from: IBM Journal of Research and Development, Vol. 54, No. 3, Paper 2
Hyperlink: N/A
Date of Publication: 2010

Abstract:
"Risk assessment methods based on scoring methods that rate the severity of each risk factor on an ordinal scale are widely used and frequently perceived by users to have value. We argue that this perceived benefit is probably illusory in most cases. We begin by describing a number of common scoring methods currently used to assess risk in a variety of different domains. We then review the literature on the use of ordinal scales in risk analysis, the use of "verbal scales" for eliciting estimates of risks and probabilities, and the extensive research about peculiar human errors when assessing risks. We also supplement this overview with some data of our own. When these diverse kinds of evidence are combined, the case against scoring methods is difficult to deny. In addition to the evidence against the value of scoring methods, there is also a lack of good evidence in their favor. We conclude our overview by reviewing the reasons why risk assessment approaches should describe risk in terms of mathematical probabilities." [p. 1]

5.7.3 What's Wrong with Hazard-Ranking Systems? An Expository Note

Title: What's Wrong with Hazard-Ranking Systems? An Expository Note
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 940-948
Retrieved from: Risk Analysis, Vol. 29, No.7
Hyperlink: N/A
Date of Publication: July 2009

Abstract:
"Two commonly recommended principles for allocating risk management resources to remediate uncertain hazards are: (1) select a subset to maximize risk-reduction benefits (e.g., maximize the von Neumann-Morgenstern expected utility of the selected risk-reducing activities), and (2) assign priorities to risk-reducing opportunities and then select activities from the top of the priority list down until no more can be afforded. When different activities create uncertain but correlated risk reductions, as is often the case in practice, then these principles are inconsistent: *priority scoring and ranking fails to maximize risk-reduction benefits.* Real-world risk priority scoring systems used in homeland security and terrorism risk assessment, environmental risk management, information system vulnerability rating, business risk matrices, and many other important applications do not exploit correlations among risk-reducing opportunities or optimally diversify risk-reducing investments. As a result, they generally make suboptimal risk management recommendations. Applying portfolio optimization methods instead of risk prioritization ranking, rating, or scoring methods can achieve greater risk-reduction value for resources spent." [p. 940]

5.7.4 What's Wrong with Risk Matrices?

Title: What's Wrong with Risk Matrices?
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 497-512
Retrieved from: Risk Analysis, Vol. 28, No. 2
Hyperlink: N/A
Date of Publication: 2008

Abstract:
"Risk matrices - tables mapping "frequency" and "severity" ratings to corresponding risk priority levels - are popular in applications as diverse as terrorism risk analysis, highway construction project management, office building risk analysis, climate change risk management, and enterprise risk management (ERM). National and international standards (e.g. Military standard 882C and AS/NZS 4360:1999) have stimulated adoption of risk matrices by many organizations and risk consultants. However, little research rigorously validates their performance in actually improving risk management decisions. This article examines some mathematical properties of risk matrices and shows that they have the following limitation. (a) *Poor Resolution*. Typical risk matrices can correctly and unambiguously compare only a small fraction (e.g., less than 10%) of randomly selected pairs of hazards. They can assign identical ratings to quantitatively very different risks ("range compression"). (b) *Errors*. Risk matrices can mistakenly assign higher qualitative ratings to quantitatively smaller risks. For risks with negatively correlated frequencies and severities, they can be "worse than useless", leading to worse-than-random decisions. (c) *Suboptimal Resource Allocation*. Effective allocation of resources to risk-reducing countermeasures cannot be based on the categories provided by risk matrices. (d) *Ambiguous Inputs and Outputs*. Categorizations of severity cannot be made objectively for uncertain consequences. Inputs to risk matrices (e.g. frequency and severity categorizations) and resulting outputs (i.e., risk ratings) require subjective interpretation, and different users may obtain opposite ratings of the same quantitative risks. These limitations suggest that risk matrices should be used with caution, and only with careful explanations of embedded judgments." [p. 497]

Key words: AS/NZS 4360; decision analysis; enterprise risk management; Military Standard 882C; qualitative risk assessment; risk matrix; semi quantitative risk assessment; worse-than-useless information

5.7.5 Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks

Title: Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1749-1761
Retrieved from: Risk Analysis, Vol. 28, No. 6
Hyperlink: N/A
Date of Publication: December 2008

Abstract:
"Several important risk analysis methods now used in setting priorities for protecting U.S. infrastructures against terrorist attacks are based on the formula: Risk = Threat × Vulnerability × Consequence. This article identifies potential limitations in such methods that can undermine their ability to guide resource allocations to effectively optimize risk reductions. After considering specific examples for the Risk Analysis and Management for Critical Asset Protection (RAMCAPTM) framework used by the Department of Homeland Security, we address more fundamental limitations of the product formula. These include its failure to adjust for correlations among its components, nonadditivity of risks estimated using the formula, inability to use risk-scoring results to optimally allocate defensive resources, and intrinsic subjectivity and ambiguity of Threat, Vulnerability, and Consequence numbers. Trying to directly assess probabilities for the actions of intelligent antagonists instead of modeling how they adaptively pursue their goals in light of available information and experience can produce ambiguous or mistaken risk estimates. Recent work demonstrates that two-level (or few-level) hierarchical optimization models can provide a useful alternative to Risk = Threat × Vulnerability × Consequence scoring rules, and also to probabilistic risk assessment (PRA) techniques that ignore rational planning and adaptation. In such two-level optimization models, defender predicts attacker's best response to defender's own actions, and then chooses his or her own actions taking into account these best responses. Such models appear valuable as practical approaches to antiterrorism risk analysis." [p. 1749]

Key words: Game theory; hierarchical optimization; RAMCAP; rational opponent; terrorism risk assessment; two-level optimization

5.7.6 Some Limitations of Qualitative Risk Rating Systems

Title: Some Limitations of Qualitative Risk Rating Systems
Author(s): Louis Anthony (Tony) Cox, Jr., Djangir Babayev, and William Huber
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 651-662
Retrieved from: Risk Analysis, Vol. 25, No. 3
Hyperlink:http://www.evira.fi/attachments/english/research_on_animal_diseases_and_food/risk_assessment/qualitative.pdf
Date of Publication: June 2005

Abstract:
"Qualitative systems for rating animal antimicrobial risks using ordered categorical labels such as "high," "medium," and "low" can potentially simplify risk assessment input requirements used to inform risk management decisions. But do they improve decisions? This article compares the results of qualitative and quantitative risk assessment systems and establishes some theoretical limitations on the extent to which they are compatible. In general, qualitative risk rating systems satisfying conditions found in real-world rating systems and guidance documents and proposed as reasonable make two types of errors: (1) Reversed rankings, i.e., assigning higher qualitative risk ratings to situations that have lower quantitative risks; and (2) Uninformative ratings, e.g., frequently assigning the most severe qualitative risk label (such as "high") to situations with arbitrarily small quantitative risks and assigning the same ratings to risks that differ by many orders of magnitude. Therefore, despite their appealing consensus building properties, flexibility, and appearance of thoughtful process in input requirements, qualitative rating systems as currently proposed often do not provide sufficient information to discriminate accurately between quantitatively small and quantitatively large risks. The value of information (VOI) that they provide for improving risk management decisions can be zero if most risks are small but a few are large, since qualitative ratings may then be unable to confidently distinguish the large risks from the small. These limitations suggest that it is important to continue to develop and apply practical quantitative risk assessment methods, since qualitative ones are often unreliable." [p. 651]

Additional Information:
This paper includes discussions on:

- Overview of some existing qualitative risk rating systems
- Theoretical analysis of risk rating approaches
- What should be done instead

Recommendations:

- "In summary, we propose that for practical risk assessment work, simple quantitative models such as product-form models (or, more generally, comparisons of sums and differences of products) with data driven upper-bound and/or lower-bound estimates of the components of the products will often be more accurate and useful than qualitative risk rating, while requiring no more information than would be needed to assess, justify, and interpret qualitative ratings." [p. 659]

5.7.7 Limits to Science for Assessing and Managing Environmental Health Risks

Title: Limits to Science for Assessing and Managing Environmental Health Risks
Author(s): Dr. Steve E. Hrudey
Organization: Canadian Institute for the Administration of Justice
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 127-150
Retrieved from: Science, Truth and Justice Conference, Article # 563
Hyperlink: N/A
Date of Publication: 2000

Purpose:

- "This paper discusses the concept of risk in the context of regulation and public policy. This paper aims to explore "what science can and cannot provide as foundations to a risk-based decision-making rationale." [p. 129]

Additional Information:
This paper includes discussions on:

- What is risk, and its implications for decision-making
- Cautions and realities of risk
- Using risk wisely

5.8 Evolution of Risk, Review of Existing Practices, Gap Analysis, Recommendations, and Future Directions

5.8.1 Mathematics of Risk and Reliability: A Select History

Title: Mathematics of Risk and Reliability: A Select History
Author(s): Nozer D. Singpurwalla, Simon P. Wilson
Organization: N/A
Publisher: Wiley
Publishing Location: Unavailable
Edition: N/A
Pages: 8
Retrieved from: Encyclopedia of Quantitative Risk Analysis and Assessment
Hyperlink: http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0485/pdf
Date of Publication: 2008

Abstract:
"This article is a brief description of some landmark advances in the mathematics of risk and reliability, starting with the initial developments of probability theory in the seventeenth century to the ascendancy of reliability theory during the last 60 years.[26]"

Keywords: decision theory; insurance; subjective probability; risk; reliability; utility

Additional Information:
This paper is divided into the following sections:

- Until 1750: The Foundations of Probability
- 1750-1900: Probability Matures
- From 1900 to the Present: Utility and Reliability Enter

[26]From http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0485/abstract

5.8.2 Three Decades of Risk Research: Accomplishments and New Challenges

Title: Three Decades of Risk Research: Accomplishments and New Challenges
Author(s): Ortwin Renn (Center of Technology Assessment, Industriestrasse)
Organization: N/A
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 49-71
Retrieved from: Journal of Risk Research Vol. 1, No. 1
Hyperlink: N/A
Date of Publication: 1998

Abstract:
"Risk research over the last three decades has been focused on the development of methods of and procedures for risk analysis and risk management. As a consequence of this research, risk management agencies have been trying to make risk assessments a routine operation for evaluating different hazards, chemical agents, or technologies. The problem with the worldwide routinization of the risk assessment methodology is, however, that formal analysis may obscure the conceptual foundations and limitations of this method and may induce a false degree of certainty when dealing with potential side-effects of human actions and interventions. One of the main tasks of the risk community should be to emphasize the necessity of integrated risk assessment and the development of innovative risk management strategies that build upon the insights of the natural, technical and social sciences. In order to integrate risk assessment and risk perception, the article analyses the strengths and weaknesses of each approach to risk analysis and highlights the potential contributions that the technical sciences and the social sciences can offer to risk management. Technical assessments provide the best estimate for judging the average probability of an adverse effect linked to an object or activity. Public perception should govern the selection of criteria on which acceptability or tolerability are to be judged. In addition, public input is needed to determine the trade-offs between criteria. Finally, public preferences are needed to design resilient strategies for coping with remaining uncertainties." [p. 49]

Additional Information:
This paper contains the following sections:

- "What is the meaning of the term 'risk'?" [p. 50]
- "The past as a guidebook for the future: technical risk assessments" [p. 52]
- "A critical review of the technical concepts and challenges for the future" [p. 53]
- "A new perspective: risk is what m" [p. 55]
- "Risk perception: the wisdom of the lay public" [p. 57]
- "A further complication: social learning of risk and institutional response" [p. 61]
- "Where to go from here: an attempt to integrate risk concepts" [p. 64]

5.8.3 OECD Studies in Risk Management - Innovation in Country Risk Management

Title: OECD Studies in Risk Management - Innovation in Country Risk Management
Author(s): Unavailable
Organization: Organisation for Economic Co-operation and Development (OECD)
Publisher: Organisation for Economic Co-operation and Development (OECD)
Publishing Location: Unavailable
Edition: Unavailable
Pages: 47
Retrieved from: Organisation for Economic Co-operation and Development (OECD) website
Hyperlink: http://www.oecd.org/dataoecd/33/18/42226946.pdf
Date of Publication: 2009

Scope:

- "Risk management of large scale events such as natural catastrophes, terrorist events and pandemic disease that pose grave consequences for a country's population and national assets...In particular, the report focuses on organisational improvements and challenges to the pre-event phases of risk management: risk identification, assessment, and mitigation activities (including both prevention and protection measures)." [p. 5]

Description:

- "This OECD report looks at innovative practices in the management of risk in six countries: the United Kingdom, Canada, the United States, Japan, the Netherlands and Singapore. It focuses on recent developments in risk management at central government level such as approaches to multi-risk identification and assessment, and methods to prioritise investments in mitigation activities." [p. 4]
- "This pamphlet provides a synthesis view of all-hazards risk management institutions and policies in the six countries under study. It points out common approaches in country risk management, such as structures to improve channels of communication between policymakers and stakeholders, and illustrates innovative tools for the use and validation of risk assessment and mitigation. Conclusions are provided to highlight challenges that the six countries continue to confront in their efforts to implement recently adopted reforms as well as opportunities to further enhance efforts already underway." [p. 6]

5.8.4 DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs: Problem Formulation and Solution Strategy

Title: DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Programs: Problem Formulation and Solution Strategy
Author(s): Lynne Genik and Paul Chouinard
Organization: Defence Research and Development Canada (DRDC) – Centre for Security Science (CSS)
Publisher: Defence Research and Development Canada (DRDC) – Centre for Security Science (CSS)
Publishing Location: Canada
Edition: N/A
Pages: 66
Retrieved from: DRDC CSS Technical Memorandum DRDC CSS TM 2012-015
Date of Publication: October 2012

Abstract:
"This paper presents the problem formulation and solution strategy component of the EMBC-DRDC collaborative project agreement for improving EMBC's Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure (CI) Assurance Programs. The methodology is described; the NATO Code of Best Practice for C2 Assessment and a soft operations research approach were applied, along with aspects of capability based planning, systems engineering, and risk management. Preliminary literature searches were performed and are documented here. Stakeholder groups are described and the questions used to elicit their perspectives on the programs and related issues are presented. The result of the analysis was the identification of program requirements, gaps, and proposed projects by DRDC to address aspects of the gaps. The proposed projects include adapting the Major Events Security Framework for use by EMBC, CI assessment tool development through pilot projects, and contracts for a community resilience framework and scenario mission to task templates, among several others." [p. i]

Note: This paper describes the background and context for the EMBC-DRDC collaborative project which is referenced in this literature search.

5.8.5 Review of the Department of Homeland Security's Approach to Risk Analysis

Title: Review of the Department of Homeland Security's Approach to Risk Analysis
Author(s): Committee to Review the Department of Homeland Security's Approach to Risk Analysis
Organization: National Research Council
Publisher: National Academies Press
Publishing Location: Washington, D.C.
Edition: N/A
Pages: 160
Retrieved from: National Academies Press website
Hyperlink: http://www.nap.edu/catalog.php?record_id=12972
Date of Publication: 2010

Description:

- "In response to a request of the U.S. Congress…, the National Research Council (NRC) established the Committee to Review the Department of Homeland Security's Approach to Risk Analysis, in order to assess how the Department of Homeland Security (DHS) is building its capabilities in risk analysis to inform decision making." [p.1]
- This report presents the Committee's findings and recommendations.
- More specifically, the study addressed the following tasks:
    a) "Evaluate the quality of the current DHS approach to estimating risk and applying those estimates in its many management, planning, and resource allocation (including grant-making) activities, through review of a committee-selected sample of models and methods
    b) Assess the capability of DHS risk analysis methods to appropriately represent and analyze risks from across the Department's spectrum of activities and responsibilities, including both terrorist threats and natural disasters
    c) Assess the capability of DHS risk analysis methods to support DHS decision-making
    d) Review the feasibility of creating integrated risk analyses covering the entire DHS program areas, including both terrorist threats and natural disasters, and make recommendations for best practices, including outreach and communications; and
    e) Recommend how DHS can improve its risk analyses and how those analyses can be validated and provide improved decision support." [p. 2]

Additional Information:
The Committee to Review the Department of Homeland Security's Approach to Risk Analysis approached the study by examining six risk analysis models and processes. They are:

- Risk analysis of natural hazards
- Risk analysis for critical infrastructure protection
- Risk analysis for allocation of homeland security grants
- Terrorism Risk Assessment and Management (TRAM) model
- Biological Threat Risk Assessment (BTRA) model
- DHS's Integrated Risk Management Framework.

5.8.6 Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change

Title: Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change
Author(s): Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis
Organization: National Research Council
Publisher: National Academies Press
Publishing Location: Washington, D. C
Edition: N/A
Pages: 172
Retrieved from: National Academies Press website
Hyperlink: http://www.nap.edu/catalog.php?record_id=12206#description
Date of Publication: 2008

Purpose:

- "Provide an independent, scientific peer review of the methodology that led to the BTRA of 2006 and that will be the foundation for future biennial updates." [p. 1]

Description:

- "The Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis was established by the National Research Council and convened in August 2006 to review the Department of Homeland Security's (DHS's) Biological Threat Risk Assessment (BTRA) of 2006. The BTRA is a computer-based tool that has been applied by DHS to assess the risk associated with the intentional release of each of 28 biological threat agents categorized by the Centers for Disease Control and Prevention…
- The committee has identified a number of fundamental concerns with the BTRA of 2006, ranging from mathematical and statistical mistakes that have corrupted results, to unnecessarily complicated probability models and models with fidelity far exceeding existing data, to more basic questions about how terrorist behavior should be modeled. All of these issues are covered in the body of this report.
- Rather than merely criticizing what was done in the BTRA of 2006, the committee sought outside experts and collected a number of proposed alternatives that it believes would improve DHS's ability to assess potential terrorist behavior as a key element of risk-informed decision making, and it explains these alternatives in the specific context of the BTRA and the bioterrorism threat." [p. 1]

5.8.7 The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress

Title: The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress
Author(s): Todd Masse, Siobhan O'Neil, John Rollins
Organization: Congressional Research Service
Publisher: Congressional Research Service
Publishing Location: United States of America
Edition: N/A
Pages: 33
Retrieved from: U.S. Department of State, Foreign press Centers website
Hyperlink: http://fpc.state.gov/documents/organization/80208.pdf
Date of Publication: February 2, 2007

Description:
"This report begins with an overview of the evolution of risk assessment methodologies from the Department of Justice in FY2002 to DHS in FY2007, and then discusses the discipline of risk management and risk assessment as applied to Homeland Security Grant Program (HSGP)." [Summary]

5.8.8 Blackett Review of High Impact Low Probability Risks

Title: Blackett Review of High Impact Low Probability Risks
Author(s): Government Office for Science
Organization: Government Office for Science
Publisher: Government Office for Science
Publishing Location: United Kingdom
Edition: Unavailable
Pages: 46
Retrieved from: Department for Business Innovation & Skills website, UK government
Hyperlink: http://www.bis.gov.uk/assets/goscience/docs/b/12-519-blackett-review-high-impact-low-probability-risks
Date of Publication: 2011

Background:

- This Blackett Review was established at the request of the Ministry of Defence (MOD) and the Cabinet Office (CO).

Purpose:

- This review addresses the issue of "High Impact Low Probability Risks" while considering the latest approaches to risk management and bringing together an expert view.
- It aims to "encapsulate the key issues and particularly highlights contemporary thinking in the field." [p. 8]

Description:

- This review focuses on four aspects of risk management. They are:
    - Emerging risk identification
    - Assessing and representing risk
    - Managing risk
    - Communicating the risk
- For each of these sections, the review provides a discussion of key concepts, existing practices, challenges and limitations, and recommendations.

Additional Information:

- The recommendations are a key component of this Blackett Review. These recommendations are aimed for government departments and agencies, as well as the cabinet office.
- They "build on existing practice, with an emphasis on refreshed thinking in a number of areas. The most notable over-arching factor in these recommendations is the repeated need for the inclusion of external experts and readiness to consider unlikely risks. Additionally, the report makes clear that behavioural matters and the role of social science in risk management needs to be enhanced." [p. 7]

5.8.9 Learning Lessons from the 2007 Floods

Title: Learning Lessons from the 2007 Floods
Author(s): Pitt Review: Sir Michael Pitt (Independent Chair), and the Review Team
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 505
Retrieved from: UK Government National Archives website
Hyperlink:
http://webarchive.nationalarchives.gov.uk/20100807034701/http:/archive.cabinetoffice.gov.uk/pittreview/thepittreview/final_report.html
Date of Publication: June 25, 2008

Description:

- This document is Sir Michael Pitt's final report, which provides a comprehensive review of the lessons to be learned from the summer floods of 2007. This document is divided into sections which reflect the 6 major lessons learned. They are:
    - "Knowing where and when it will flood
    - Reducing the risk of flooding and its impact
    - Being rescued and cared for during an emergency
    - Maintaining power and water supplies and protecting essential services
    - Better advice and help for people to protect their families and homes
    - Staying healthy and speeding up recovery." [p. viii]
- For each of these sections, this report offers recommendations for how the country can improve preparation, response and recovery for flooding.

Additional Information:
For those interested in risk assessment, Section 2, *Knowing when and where it will flood* is most relevant. It contains sections on:

- International Context: Different approaches to risk and the impact of flooding
- Overview of risk: Examines current and future approaches for managing flood risk
- Forecasting, modelling and mapping: Examines the science and technology behind these processes

5.8.10 Risk Assessment Tools, Techniques and Data for the Civil Contingencies Act and Integrated Risk Management Planning

Title: Risk Assessment Tools, Techniques and Data for the Civil Contingencies Act and Integrated Risk Management Planning
Author(s): Department for Communities and Local Government
Organization: Department for Communities and Local Government
Publisher: Communities and Local Government Publications
Publishing Location: Wetherby, UK
Edition: N/A
Pages: 195
Retrieved from: Fire Research Series 5/2008, Communities and Local Government website
Hyperlink: http://www.communities.gov.uk/documents/fire/pdf/Riskassessmenttools.pdf
Date of Publication: May 2008

Purpose:

- "Research and produce advice on the availability, selection and use of risk assessment tools, techniques, data and guidance to support the obligations of LRFs [Local Resilience Forums] under the Civil Contingencies Act 2004 and risk analysis for IRMPs [Integrated Risk Management Plan]." [p. 3]

Description:
This report presents the findings for every phase of this project:

- Consultation with the Local Resilience Forums and the Fire Rescue Services regarding:
  - Local Resilience Forum's (LRF) civil contingencies risk assessment
  - Integrated Risk Management Plan (IRMP)-specific risk analysis
- Gap analysis
- Filling the gaps: data, tools, techniques
- Conclusions and recommendations

5.8.11 Natural Hazards in Australia: Identifying Risk Analysis Requirements

Title: Natural Hazards in Australia: Identifying Risk Analysis Requirements
Author(s): Miriam H. Middelmann (Ed.) (Risk and Impact Analysis Group, Geospatial and Earth Monitoring Division, Geoscience Australia)
Organization: Geoscience Australia, Australian Government
Publisher: Geoscience Australia
Publishing Location: Canberra, AU
Edition: N/A
Pages: 206
Retrieved from: Pacific Disaster website
Hyperlink: http://www.pacificdisaster.net/pdnadmin/data/original/AUS_GA_Natural_hazards.pdf
Date of Publication: 2007

Purpose:

- "The purpose of this Report is to provide a knowledge base of how to conduct a risk analysis for natural hazards in Australia.
- The Report considers the suite of natural hazards identified by COAG [Council of Australian Government] and addresses a range of issues including impacts, gaps, data requirements and risk analyses. The report highlights the gains in a long-term data collection system and how integral it is to the risk analysis process." [p. ii]

Audience:

- "Those who have an interest in, or a responsibility for, the management of natural hazards and the reduction of their impacts." [p. 4]

Description:

- This report begins with a discussion on:
    - Impact of natural disasters
    - Brief introduction to risk analysis
- The report then discusses hazard identification, cost, risk analysis, information gaps, and roles and responsibilities for each of the following hazards:
    - Tropical Cyclone
    - Flood
    - Severe Storm
    - Bushfire
    - Landslide
    - Earthquake
    - Tsunami Events

5.8.12 Converging Physical and Information Security Risk Management

Title: Converging Physical and Information Security Risk Management
Author(s): Syed (Shawon) M. Rahman and Shannon E. Donahue
Organization: N/A
Publisher: The Conference Board
Publishing Location: United States of America
Edition: N/A
Pages: 6
Retrieved from: The Conference Board, Executive Active Series, No. 344
Hyperlink: N/A
Date of Publication: February 2011

Abstract:
"Traditionally, physical and information security have operated in their own silos with separate teams and different risks, processes, and budgets. But risks and threats are evolving and becoming interdependent. As new technologies are adopted in the workplace, the company risk profile expands. Theft of intellectual property, risks in the supply chain, and other issues of the extended enterprise are forcing businesses to take a more holistic approach." [p. 1]

Additional Information:
This paper discusses the following topics:

- Benefits of Convergence
- Challenges of Convergence (Role of culture, Organization of the Security Function)
- Enterprise Risk management

**Editor's Note:* "This Executive Action is based upon the authors' article "Convergence of Corporate and Information Security" published in the *International Journal of Computer Science and Information Security,* Vol. 7, No. 1, 2010 and previous research by The Conference Board." [p. 1]

5.8.13 Convergence of Corporate and Information Security

Title: Convergence of Corporate and Information Security
Author(s): Syed (Shawon) M. Rahman, PhD. and Shannon E. Donahue CISM, CISSP
Organization: N/A
Publisher: International Journal of Computer Science and Information Security (IJCSIS) Publication
Publishing Location: Unavailable
Edition: N/A
Pages: 63-68
Retrieved from: International Journal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 1
Hyperlink: http://arxiv.org/ftp/arxiv/papers/1002/1002.1950.pdf
Date of Publication: 2010

Abstract:
"As physical and information security boundaries have become increasingly blurry many organizations are experiencing challenges with how to effectively and efficiently manage security within the corporate. There is no current standard or best practice offered by the security community regarding convergence; however many organizations such as the Alliance for Enterprise Security Risk Management (AESRM) offer some excellent suggestions for integrating a converged security program. This paper reports on how organizations have traditionally managed asset protection, why that is changing and how to establish convergence to optimize security's value to the business within an enterprise." [p. 63]

Keywords: component; convergence; security; risk management; corporate; threats

Additional Information:
This paper covers the following topics:

- Reasons for Convergence
- Benefits of Convergence
- Challenges of Convergence
- Beginning a Converged Program

5.9 Risk Assessment for Terrorism - Challenges and Applicability of Existing methods

5.9.1 How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts

Title: How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts
Author(s): Gerald G. Brown and Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 196-204
Retrieved from: Risk Analysis, Vol. 31, No. 2
Hyperlink: N/A
Date of Publication: February 2011

Abstract:
"Traditional probabilistic risk assessment (PRA), of the type originally developed for engineered systems, is still proposed for terrorism risk analysis. We show that such PRA applications are unjustified in general. The capacity of terrorists to seek and use information and to actively research different attack options before deciding what to do raises unique features of terrorism risk assessment that are not adequately addressed by conventional PRA for natural and engineered systems—in part because decisions based on such PRA estimates do not adequately hedge against the different probabilities that attackers may eventually act upon. These probabilities may differ from the defender's (even if the defender's experts are thoroughly trained, well calibrated, unbiased probability assessors) because they may be conditioned on different information. We illustrate the fundamental differences between PRA and terrorism risk analysis, and suggest use of robust decision analysis for risk management when attackers may know more about some attack options than we do." [p. 196]

Description:

- This paper considers "why a belief that there is no fundamental difference in conditional probability calculations for systems with and without reasoning agents can provide a dangerously misleading foundation for terrorism risk analysis." [p. 197]
- The key arguments are as follows:
    - "Attack risks may depend on the defender's risk analysis results" [p. 197]
    - "PRA for terrorist attacks may recommend poor risk management decisions...because attack probabilities depend on what the attacker knows or believes, rather than on what the defender knows or believes." [p. 198]
    - "The irrelevance of defender information to predicting how defenses affect risk" [p. 201]
- This paper then discusses the practical implications for U.S. terrorism risk management, then recommends the following:
    - "Making robust risk management decisions that acknowledge that the attacker may know things we do not…
    - Shifting the emphasis of risk management from using experts to guess where risk might be greatest...to calculating where targeted investments will most improve the resilience of critical infrastructures." [p. 204]

5.9.2 Probabilistic Risk Analysis and Terrorism Risk

Title: Probabilistic Risk Analysis and Terrorism Risk
Author(s): Barry Charles Ezell, Steven P. Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 575-589
Retrieved from: Risk Analysis, Vol. 30 No. 4
Hyperlink: http://www.dhs.gov/xlibrary/assets/rma-risk-assessment-technical-publication.pdf
Date of Publication: April 2010

Abstract:
"Since the terrorist attacks of September 11, 2001, and the subsequent establishment of the U.S. Department of Homeland Security (DHS), considerable efforts have been made to estimate the risks of terrorism and the cost effectiveness of security policies to reduce these risks. DHS, industry, and the academic risk analysis communities have all invested heavily in the development of tools and approaches that can assist decisionmakers in effectively allocating limited resources across the vast array of potential investments that could mitigate risks from terrorism and other threats to the homeland. Decisionmakers demand models, analyses, and decision support that are useful for this task and based on the state of the art. Since terrorism risk analysis is new, no single method is likely to meet this challenge. In this article we explore a number of existing and potential approaches for terrorism risk analysis, focusing particularly on recent discussions regarding the applicability of probabilistic and decision analytic approaches to bioterrorism risks and the Bioterrorism Risk Assessment methodology used by the DHS and criticized by the National Academies and others." [p. 575]

Background:

- This paper is a response to recent criticism of probabilistic risk assessment approaches to terrorism risk analyses (especially those made by the National Research Council's Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis).

Purpose:

- "Justify the use of PRA for terrorism risk analysis, while acknowledging its limitations…
- To propose a pluralistic approach to terrorism risk analysis, which allows alternative approaches to be examined and tested. To this end, we examine some alternative approaches and discuss their contributions and limitations. While we do not take issue here with the possible value of these alternative approaches, we aim to make a case that (1) probabilities of terrorism events are useful to assess terrorism risks; (2) event trees can be used as part of a terrorism PRA to decompose the universe of terrorism scenarios; and (3) alternatives suggested by the NRC Committee like extended forms of games or decision trees constructed from the terrorists' perspective, like all approaches, have limitations." [p. 576]

5.9.3 Game Theory and Risk Analysis

Title: Game Theory and Risk Analysis
Author(s): Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1062-1068
Retrieved from: Risk Analysis, Vol. 29, No. 8
Hyperlink: N/A
Date of Publication: August 2009

Abstract:
"Risk analysts often analyze adversarial risks from terrorists or other intelligent attackers without mentioning game theory. Why? One reason is that many adversarial situations—those that can be represented as *attacker-defender games*, in which the defender first chooses an allocation of defensive resources to protect potential targets, and the attacker, knowing what the defender has done, then decides which targets to attack—can be modeled and analyzed successfully without using most of the concepts and terminology of game theory. However, risk analysis and game theory are also deeply complementary. Game-theoretic analyses of conflicts require modeling the probable consequences of each choice of strategies by the players and assessing the expected utilities of these probable consequences. Decision and risk analysis methods are well suited to accomplish these tasks. Conversely, game-theoretic formulations of attack-defense conflicts (and other adversarial risks) can greatly improve upon some current risk analyses that attempt to model attacker decisions as random variables or uncertain attributes of targets ("threats") and that seek to elicit their values from the defender's own experts. Game theory models that clarify the nature of the interacting decisions made by attackers and defenders and that distinguish clearly between strategic *choices* (decision nodes in a game tree) and random variables (*chance* nodes, not controlled by either attacker or defender) can produce more sensible and effective risk management recommendations for allocating defensive resources than current risk scoring models. Thus, risk analysis and game theory are (or should be) mutually reinforcing." [p. 1062]

5.9.4 Applying the General Theory of Quantitative Risk Assessment (QRA) to Terrorism Risk

Title: Applying the General Theory of Quantitative Risk Assessment (QRA) to Terrorism Risk
Author(s): Stan Kaplan (Center for Risk Management of Engineering Systems, University of Virginia)
Organization: N/A
Publisher: American Society of Civil Engineers (ASCE)
Publishing Location: Unavailable
Edition: N/A
Pages: 77-81
Retrieved from: Proceedings of 10th United Engineering Foundation Conference
Hyperlink: N/A
Date of Publication: 2004

Abstract:
"The purpose of this paper is to point out that the general theory of quantitative risk assessment (QRA) applies perfectly well to evaluating and quantifying the risk from terrorism. The main difference occurs during the 'scenario identification' part of the risk assessment process. Whereas, in an "ordinary" QRA, we ask the question, "What can go wrong?," in terrorism risk assessment (TQRA) we ask, "If I wanted to, what could I make go wrong?" In answering this new question, the Theory of Scenario Structuring and the use of fault and event trees play the major roles as before. Also, the concept of "resources" now moves to center stage as part of the process of identifying terrorism scenarios. So also does the use of Bayes' theorem, not only to assess *a priori* the likelihoods of specific terrorism scenarios, but also as a crucial part of surveillance systems that have, potentially, the ability to quantify the likelihoods that such scenarios are in process." [p. 77]

5.9.5 Is ALARP Applicable to the Management of Terrorist Risks?

Title: Is ALARP Applicable to the Management of Terrorist Risks?
Author(s): S.D. Guikema, T. Aven
Organization: N/A
Publisher: Elsevier ltd.
Publishing Location: Unavailable
Edition: N/A
Pages: 823-827
Retrieved from: Reliability Engineering and System Safety, Vol. 95, No. 8
Hyperlink: N/A
Date of Publication: August 2010

Abstract:
"In this paper, we discuss the applicability of the as low as reasonably practicable (ALARP) principle to terrorist risk management. ALARP is a commonly used framework for managing risk due to non-intelligent threats, but terrorism introduces difficult issues, both technically and socially. In particular, the probability of a terrorist attack is difficult to define, terrorist threats are adaptive, and some terrorist risk management actions raise issues of loss of civil liberties not raised by risk management measures for other types of risk. We discuss these issues and their implications for risk management. After showing how ALARP is used to manage the risk from other hazards in different economic sectors, we discuss both the benefits and difficulties associated with extending the ALARP framework for terrorist risk analysis. We conclude that the ALARP framework can be modified to make it appropriate for risk management for adaptive risks, provided that care is taken to explicitly consider adaptive reallocation of risk in response to risk management actions, to account for perceived or actual loss of civil liberties resulting from risk management actions, and to consider the difficulties associated with using probability to measure uncertainty in adversary actions." [p. 823]

Additional Information:
This paper is structured as follows:

- "We begin by providing an overview of the application of ALARP for threats of a safety risk nature.
- We then discuss the differences between adaptive and safety risk threats in more detail before presenting a framework for how ALARP can be used within the adaptive threat setting.
- We close with a discussion of the advantages, disadvantages, and challenges of using ALARP to manage risks of an adaptive nature." [p. 823]

5.9.6 Response: Making Terrorism Risk Analysis Less Harmful and More Useful: Another Try

Title: Response: Making Terrorism Risk Analysis Less Harmful and More Useful: Another Try
Author(s): Gerald G. Brown and Louis Anthony (Tony) Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: N/A
Edition: N/A
Pages: 193-195
Retrieved from: Risk Analysis, Vol. 31, No. 2
Hyperlink: N/A
Date of Publication: February 2011

Background:

- This paper is a response to Ezell et al's criticisms.

Description:
The authors reiterate and clarify their reasoning on the following topics:

- "Intelligence analysts cannot condition on knowledge that they do not have." [p. 193]
- "Simple examples suffice for proofs by contradiction." [p. 193]
- "The poor performance of expert judgments about future political and conflict events is well established by empirical studies." [p. 193]
- "Poor risk analysis threatens us all." [p. 194]
- "Better risk analysis is easy." [p. 194]

5.9.7 Are Risk Assessments of a Terrorist Attack Coherent?

Title: Are Risk Assessments of a Terrorist Attack Coherent?
Author(s): David R. Mandel (Defence Research and Development Canada and University of Toronto)
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 277-288
Retrieved from: Journal of Experimental Psychology: Applied, Vol. 11, No. 4
Date of Publication: 2005

Abstract:
"Four experiments examined 3 types of violations of coherence criteria in risk assessments of a terrorist attack. First, the requirement that extensionally equivalent descriptions be assigned the same probability (i.e., additivity) was violated. Unpacking descriptions of an attack into subtypes led to an increase in assessed risk. Second, additivity was also violated when risk assessments were obtained by subtracting the probability of no attack from 1.0. This refocusing procedure inflated assessed risk. Third, refocusing also increased the proportion of monotonicity violations in assessing risk across increasing or decreasing timeframes. Task structuring that promoted consideration of complementary possibilities increased coherence, suggesting that incoherence is due primarily to errors in applying rather than comprehending the relevant criteria." [p. 277]

Keywords: Risk forecasting; coherence violations; additivity; terrorism

Note: This article also appears as a DRDC-Toronto publication: DRDC-TORONTO-SL-2005-081

5.9.8 Testimony: Challenges of Applying Risk Management to Terrorism Security Policy

Title: Testimony: Challenges of Applying Risk Management to Terrorism Security Policy
Author(s): Henry H. Willis
Organization: RAND Corporation
Publisher: RAND Corporation
Publishing Location: United States of America
Edition: N/A
Pages: 10
Retrieved from: RAND Corporation Testimony Series, Testimony submitted for the record to the House Homeland Security Committee, Subcommittee on Transportation Security and Infrastructure Protection
Hyperlink: N/A
Date of Publication: June 2008

Description:
This testimony discusses the following topics:

- "Risk Analysis Provides Structure to Decisionmaking" [p. 2]
- "Challenges of Assessing Terrorism Risk" [p. 3]
- "Challenges of Assessing Terrorism Risk Management Alternatives" [p. 4]
- "Building Capacity for Risk Informed Decisionmaking at DHS" [p. 5]
- "Risk Analysis Can Help DHS Improve Terrorism Security" [p. 6]

5.9.9 Improving Risk-Based Decision Making for Terrorism Applications

Title: Improving Risk-Based Decision Making for Terrorism Applications
Author(s): Louis Anthony Cox, Jr.
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 336-341
Retrieved from: Risk Analysis, Vol. 29, No. 3
Hyperlink: N/A
Date of Publication: March 2009

Abstract:
"How can we best allocate limited defensive resources to reduce terrorism risks? Dillon *et al*.'s Antiterrorism Risk-Based Decision Aid (ARDA) system provides a useful point of departure for addressing this crucial question by exhibiting a real-world system that calculates risk reduction scores for different portfolios of risk-reducing countermeasures and using them to rank-order different possible risk mitigation alternatives for Navy facilities. This comment points out some potential limitations of any scoring system that does not take into account risk externalities, interdependencies among threats, uncertainties that are correlated across targets, and attacker responses to alternative allocations of defensive resources. In at least some simple situations, allocations based on risk reduction scores and comparisons can inadvertently *increase* risks by providing intelligent attackers with valuable information, or they can fail to reduce risks as effectively as non-scoring, optimization-based approaches. These limitations of present scoring methods present exciting technical challenges and opportunities for risk analysts to develop improved methods for protecting facilities and infrastructure against terrorist threats." [p. 336]

5.9.10 Estimating Terrorism Risk

Title: Estimating Terrorism Risk
Author(s): Henry H. Willis, Andrew R. Morral, Terrence K. Kelly, Jamison Jo Medby
Organization: RAND Center for Terrorism Risk Management Policy
Publisher: RAND Corporation
Publishing Location: Saint Monica, CA; Arlington, VA; Pittsburgh, PA
Edition: N/A
Pages: 94
Retrieved from: N/A
Hyperlink: N/A
Date of Publication: 2005

Audience: "Federal, state, local, and private sector officials responsible for estimating terrorism risks and providing guidance on resource allocation and prioritization based upon these risk estimates." [p. viii]

Description:

- "This monograph examines several challenges to risk-based allocation of homeland security resources. There is not a consistent and shared definition of terrorism risk. Estimating terrorism risk requires treatment of numerous, large uncertainties. There is no existing framework for selecting and combining risk indicators. Finally, little work has been directed toward methods for testing how the accuracy and distribution of risk from different estimates change with respect to a wide range of assumptions about terrorist threats and capabilities and the dearth of information about how security investments might reduce terrorism risk. This monograph addresses each of these issues and proposes solutions to all except the final one, understanding the relationship between investment and risk reduction, which—though a critical problem—has been left for further study." [p. vii]
- This document includes the following sections:
    - "Terrorism risk and its components…
    - Accounting for uncertainty and values in terrorism risk…
    - Two approaches to estimating terrorism risk in urban areas…
    - Evaluating the performance of different estimates…
    - Conclusions and recommendations" [p. ix]

Additional Information:
Five recommendations for improving the allocation of homeland security measures:

1. "DHS should consistently define terrorism risk in terms of expected annual consequences
2. DHS should seek robust risk estimators that account for uncertainty about terrorism risk and variance in citizen values
3. DHS should develop event-based models of terrorism risk, like that used by RAND and RMS.
4. Until reliable event- based models are constructed, density-weighted population should be preferred over population as a simple risk indicator
5. DHS should fund research to bridge the gap between terrorism risk assessment and resource allocation policies that are cost effective." [p. 55-56]

5.9.11 Cost Effectiveness of Risk Mitigation Strategies for Protection of Buildings against Terrorist Attack

Title: Cost Effectiveness of Risk Mitigation Strategies for Protection of Buildings against Terrorist Attack
Author(s): Mark G. Stewart
Organization: N/A
Publisher: American Society of Civil Engineers
Publishing Location: Unavailable
Edition: N/A
Pages: 115-120
Retrieved from: Journal of Performance of Constructed Facilities, Vol. 22, No. 2
Hyperlink: N/A
Date of Publication: March/April 2008

Abstract:
"The technical note considers the cost effectiveness of risk mitigation measures for protection of buildings to terrorist threats. Protective measures might include vehicle barriers, perimeter walls, blast resistant glazing, strengthened perimeter columns, etc. Indicative values of attack probability and characteristics of commercial buildings in the United States are described. The cost effectiveness of protective measures are calculated from a preliminary economic decision analysis that includes cost of the protective measures, attack probability, reduction in risk due to protective measures, and failure consequences. Economic risks due to terrorism are compared with risks from hurricane and seismic hazards." [p. 115]

Description:

- "The main issue to be addressed in the present technical note is whether the extra costs associated with blast-resistant structural design, enhanced perimeter security, facility relocation, and other protective measures are balanced by an appropriate reduction in risk. In other words, is the reduction in risk worth the additional expenditure?, which in many cases can exceed 20% of the original cost of a building (Morris et al. 1991).
- This need has led to a simplified economic analysis by Little (2007), who showed that unless the probability of attack against a specific building is high, the expected benefits are unlikely to offset the cost of protecting multiple structures, and so the “immediate and large sunk costs” of facility hardening “need to be used judiciously.” The present technical note aims to address and further refine this type of economic analysis." [p. 116]

5.9.12 Risk Acceptability and Cost-Effectiveness of Protective Measures Against Terrorist Threats to Built Infrastructure Considering Multiple Threat Scenarios

Title: Risk Acceptability and Cost-Effectiveness of Protective Measures Against Terrorist Threats to Built Infrastructure Considering Multiple Threat Scenarios
Author(s): Mark G. Stewart (Centre for Infrastructure Performance and Reliability, the University of Newcastle, AU)
Organization: N/A
Publisher: Springer-Verlag
Publishing Location: Unavailable
Edition: N/A
Pages: 313-317
Retrieved from: Transactions of Tianjin University, Vol. 14, No. 5
Hyperlink: N/A
Date of Publication: 2008

Abstract:
"Decisions are often needed about the need and/or extent of protective measures against explosive blast loads on built infrastructure. A decision support analysis considers fatality risks and cost-effectiveness of protective measures expressed in terms of expected cost spent on risk reduction per life saved for terrorist threats to infrastructure. The analysis is applicable to any item of infrastructure, but in this paper is applied to casualties arising from building facade glazing damage. Risks may be compared with risk acceptance criteria in the form of quantitative safety goals. The risk acceptability and cost-effectiveness of protective measures includes cost of the protective measures, attack probability, reduction in risk due to protective measures, probability of fatality conditional on successful terrorist attack and number of exposed individuals." [p. 313]

Keywords: risk; terrorism; cost-benefit analysis; infrastructure; decision analysis

Description:
- This paper presents an approach for assessing the risks and costs of mitigation decisions.
- The approach uses two criteria to determine risk acceptability. They are:
    - Fatality risks
    - Cost-effectiveness of protective measures, measured in terms of expected cost per life saved.

Additional Information:
This paper describes:
- Quantitative safety goals
- Measures of risk
- Illustrative example

5.10 Miscellaneous

5.10.1 Bayesian Statistics in Quantitative Risk Assessment

Title: Bayesian Statistics in Quantitative Risk Assessment
Author(s): Peter Congdon
Organization: N/A
Publisher: Wiley
Publishing Location: Unavailable
Edition: Unavailable
Pages: 17
Retrieved from: Encyclopedia of Quantitative Risk Analysis and Assessment
Hyperlink: http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0518/pdf
Date of Publication: 2008

Abstract:
"This chapter reviews some of the principles of Bayesian inference, with a focus on applications in risk assessment in various fields. The review is set in a context in which major gains in applying and estimating Bayesian models are due to improved iterative sampling techniques for estimation. Principles underlying specification of priors on parameters and also the main elements of posterior summarization are discussed. Issues of identification in more complex random-effects models as well as ways of assessing convergence of iterative sampling by Markov Chain Monte Carlo (MCMC) techniques are mentioned in this chapter. Two worked examples including WINBUGS code illustrate some of the principles discussed; these involve ozone exceedances in the first case study, and cancer risk in relation to arsenic in drinking water in the second case study.[27]"

Keywords: Markov chain Monte Carlo; prior specification; posterior inference; estimation; hierarchical; risk analysis; sensitivity; exceedance; convergence

[27] From http://onlinelibrary.wiley.com/doi/10.1002/9780470061596.risk0518/abstract

5.10.2 Determining Overall Risk

Title: Determining Overall Risk
Author(s): Scott Campbell (Department of Philosophy and Institute for the Study of Genetics, Biorisks and Society, University of Nottingham, UK)
Organization: N/A
Publisher: Routledge
Publishing Location: Unavailable
Edition: N/A
Pages: 569-581
Retrieved from: Journal of Risk Research, Vol. 8, No. 7-8
Hyperlink: N/A
Date of Publication: October-December 2005

Abstract:
"The risk journal literature lacks a clear and simple account of the conceptual issues involved in determining the overall risk of an action, and in explaining how risk is additive. This article attempts to bring a measure of clarity to these issues in as basic and non-technical a way as possible. First of all, the view that risk is 'expected harm' is explained. The view that risk is a quantitative concept is then defended. The distinction between the risk run by doing action A in respect of possible outcome x, and the overall risk run by doing action A in general is explained, as is the position that the overall risk of A is determined by summing the risks of each possible harm that A could give rise to. The article then explains how risks can be summed over time, as long as the probabilities involved are determined according to probability theory.
Finally, the article explains that in a doing a risk-benefit analysis of A, positive aspects of a possible outcome x, where x is harmful on balance, must be incorporated into x's level of harm rather than incorporated into the benefit side of the risk-benefit analysis of A." [p. 569]

Key words: risk, risk analysis; probability; harm; expected utility; risk-benefit analysis

Purpose:
- This article aims to provide a "clear and simple account of the conceptual issues involved in determining the overall risk of an action, and in explaining how risk is additive." [p. 569]

Additional Information:
The paper covers the following issues:
- Risk as harm weighted by probability
- Expected harm
- Risk as a quantitative concept
- The risk of A in general
- The additivity of risks
- Combinations of harms
- Practical difficulties
- Risks over time
- Risk-benefit analyses

5.10.3 Risk Reduction Prioritization using Decision Analysis

Title: Risk Reduction Prioritization using Decision Analysis
Author(s): Tim Bedford and John Quigley
Organization: N/A
Publisher: Taylor & Francis Ltd
Publishing Location: Oxfordshire, UK
Edition: N/A
Pages: 223-236
Retrieved from: Risk, Decision& Policy, Vol. 9, Issue 3
Hyperlink: N/A
Date of Publication: July-September 2004

Abstract:
"The ALARP principle is applied in many areas to regulate the tolerable level of risk. Usually the principle is operationalized by assigning a value per fatality. A cost-benefit analysis is used to trade the expected value of lives saved with the costs of technical measures required to reduce risks. In sectors in which risks have been reduced over a period of years, it is difficult to pinpoint those areas in which further risk reduction might be sought. In this article we show that many different risk reduction mechanisms can be considered simultaneously in a decision analysis framework. Using influence diagrams it is straightforward to build mini-decision analysis models in which competing alternatives addressing the same risk can be compared. The mini-model decision alternatives are assembled into decision strategies representing the best possible combination of alternatives at different cost/benefit ratios. Disynergies between the different alternatives are highlighted through the model. The overall aim is to build a high-level model to explore the sensitivity of risk reduction measures to the value per fatality parameter. This enables decision makers to gain a better understanding of the cost of measures required to obtain a global reduction in risk." [p. 223]

5.10.4 On the Risk Criterion and the Index of Risk

Title: On the Risk Criterion and the Index of Risk
Author(s): J.C. Wang, R.O. Johnson, and D.W. Lee
Organization: Energy Division, Oak Ridge National Laboratory Oak Ridge, Tennessee
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 16
Retrieved from: Paper submitted to International Topical Meeting on Probabilistic Safety Assessment (PSA '96)
Hyperlink: N/A
Date of Publication: June 10, 1996

Abstract:
"The development of a means to quantify risk, the determination of a risk criterion, and the establishment of a method to compare risks are three essential components in a probabilistic safety assessment. In this paper, the quantitative definition of risk given by Kaplan and Garrick is converted from a table to a graph to accommodate Farmer's method of constructing a risk criterion. Farmer's criterion is limited to a straight line, but its slope is made a free parameter. The high-frequency small-consequence problem noted by Farmer is solved by using an auxiliary vertical line to exclude scenarios with insignificant consequences. To compare risks associated with various accident scenarios, an index of risk relative to the straight-line risk criterion is proposed and developed. The results allow various accident scenarios to be ranked according to their weighted risks and, in turn, provide a measure of the effectiveness of mitigation." [p. 1]

6 Case Studies

Overview

This section includes references that present the unclassified results of risk assessments performed at the national, regional, or local level. Although some of these risk assessments consider all hazards and threats, others are hazard/threat specific and/or specific to certain sectors. This section is divided geographically according to the country in which the risk assessment was conducted. The sub-sections are as follows:

- **Section 6.1**: Canada
- **Section 6.2:** United States
- **Section 6.3:** United Kingdom
- **Section 6.4**: Australia
- **Section 6.5**: The Netherlands
- **Section 6.6**: Miscellaneous

6.1 Canada

6.1.1 Community Risk Assessment - Hazards, Vulnerabilities and Risks in: Town of Sidney

Title: Community Risk Assessment - Hazards, Vulnerabilities and Risks in: Town of Sidney
Author(s): Smart Risk Control, Inc.
Organization: Town of Sidney Emergency Program
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 56
Retrieved from: Town of Sidney website
Hyperlink: http://www.sidney.ca/Assets/Emergency+Services/Community+Risk+Assessment.pdf
Date of Publication: August 31, 2007

Description:

- "This report addresses hazards that could affect the residents and businesses of the Town of Sidney and lead to a major emergency or disaster." [p. 1]

Additional Information:

- First, this report presents a community profile which provides an overview of the demographics, infrastructure, community services, and the economy in the Town of Sidney.
- The report then discusses the 12 hazard types identified by the Emergency Planning Committee which might require significant site support. They are:
    - Atmospheric Hazards
    - Disease-Human
    - Earthquake
    - Fire, Major Urban
    - Hazardous Materials
    - Structure Collapse
    - Terrorism
    - Transportation - Road, Marine, Air
    - Tsunami
    - Utility Failure
    - Water Encroachment
    - Other Hazards
- The above hazards are assessed in terms of relative risk to the community. The report offers a description of the hazard, a qualitative risk rating, and an overview of past events, hazard areas, vulnerabilities and implications. Under the implications section, the report highlights opportunities for mitigation, emergency response, and coordinated recovery.
- Lastly, the report presents the hazards in a risk matrix, and briefly discusses priority concerns.

Note: This report will be updated at least every five years.

6.1.2 Applying the HAZUS-MH Software Tool to Assess Seismic Risk in Downtown Ottawa, Canada

Title: Applying the HAZUS-MH Software Tool to Assess Seismic Risk in Downtown Ottawa, Canada
Author(s): S.K. Ploeger, G.M. Atkinson, C. Samson
Organization: N/A
Publisher: Springer Netherlands
Publishing Location: Unavailable
Edition: N/A
Pages: 1-20
Retrieved from: Natural Hazards, Vol. 53, No. 1
Hyperlink: N/A
Date of Publication: 2010

Abstract:
"The aim of this paper is to present earthquake loss estimations for a portion of downtown Ottawa, Canada, using the HAZUS-MH (Hazards United States Multi-Hazard) software tool. The assessment is performed for a scenario earthquake of moment magnitude 6.5, at an epicentral distance of 15 km, occurring during business hours. A level 2 HAZUS-MH analysis was performed where the building inventory, microzonation studies, and site-specific ground motion hazard maps (2% exceedence probability in 50 years) were all improved based on local information. All collected data were assembled into a set of standard geodatabases that are compatible with the HAZUS-MH software using a GIS-specific procedure. The results indicate that the greatest losses are expected in unreinforced masonry buildings and commercial buildings. Sensitivity studies show that soil classes, the vulnerability of schools, and the spatial scale of loss estimations are also important factors to take into account." [p. 1]

Keywords: HAZUS; Eastern Canadian earthquakes; Loss estimations; Damage assessment; Casualty assessment; Eastern North American ground motions

6.2 United States

6.2.1 The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation

Title: The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation
Author(s): Department of Homeland Security (DHS)
Organization: Department of Homeland Security (DHS)
Publisher: Unavailable
Publishing Location: United States of America
Edition: N/A
Pages: 7
Retrieved from: Department of Homeland Security (DHS) website
Hyperlink: http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
Date of Publication: December 2011

Background:

- The Strategic National Risk Assessment (SNRA) was "executed in support of Presidential Policy Directive 8 (PPD-8), which calls for the creation of a National Preparedness Goal, a National Preparedness System, and a National Preparedness Report." [p. 1]

Scope:

- The SNRA “evaluated the risk from known threats and hazards that have the potential to significantly impact the Nation’s homeland security.” [p. 2]
- Considers all hazards and threats

Description:

- This document provides an overview of the SNRA.
- The document then provides a summary of the unclassified findings and a description of the analytic approach used for the SNRA.
- In addition, it discusses the limitations of the SNRA, as well as its impacts and future uses.

6.2.2 Annex D: All Hazard Vulnerability Assessment

Title: Annex D: All Hazard Vulnerability Assessment
Author(s): City of Livermore, California
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 85
Retrieved from: City of Livermore, California: Comprehensive Emergency Management Plan
Hyperlink: http://www.cityoflivermore.net/civicax/filebank/documents/4184/
Date of Publication: 2005

Description:
"This document describes natural and technological (human-made) hazards, which can potentially impact the people, economy, environment, and property of the City of Livermore. It serves as a basis for city-level emergency management programs. It is the foundation of effective emergency management and identifies the hazards that organizations must mitigate against, prepare for, respond to, and recover from in order to minimize the effects of disasters and emergencies. The All-Hazard Vulnerability Analysis is an overview of hazards that can cause emergencies and disasters." [p. 3]

6.3 United Kingdom

6.3.1 National Risk Register of Civil Emergencies 2012

Title: National Risk Register of Civil Emergencies 2012
Author(s): National Government (UK)
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: United Kingdom
Edition: 3rd ed. (2012)
Pages: 58
Retrieved from: Cabinet Office website
Hyperlink:
http://www.cabinetoffice.gov.uk/sites/default/files/resources/CO_NationalRiskRegister_2012_acc.pdf
Date of Publication: 2012

Purpose:

- "The *National Risk Register of Civil Emergencies* (NRR) is a reference document for individuals and organisations wishing to be better prepared for emergencies.
- This is the second revision of the NRR since its original publication in 2008, and provides updated information on the types of civil emergency that people in the UK could face over the next five years." [p.1]

Additional Information:
The Risk Register includes:

- Overview of the main types of civil emergency
    - Describes some of the highest priority risks, and displays them on risk matrices
- Risk descriptions
    - Detailed descriptions about a wide variety of risks
    - Information on how the government and emergency responders are planning to prepare for and respond to these risks.

6.3.2 National Risk Register of Civil Emergencies 2010

Title: National Risk Register of Civil Emergencies 2010
Author(s): National Government (UK)
Organization: Cabinet Office
Publisher: Cabinet Office
Publishing Location: United Kingdom
Edition: 2nd edition (2010)
Pages: 58
Retrieved from: Cabinet Office website
Hyperlink:
http://www.cabinetoffice.gov.uk/sites/default/files/resources/nationalriskregister-2010.pdf
Date of Publication: 2010

Audience:

- "The National Risk Register is intended for those who want to improve their ability to respond to emergencies." [p.2]

Description:

- The National Risk Register (NRR) provides a description of a variety of risks that the UK can face over the next five years.
- It also provides information on how the government and emergency responders are preparing in the case that these risks materialize.
- In addition, the NRR provides guidance for businesses, organizations, families, and communities to prepare for emergencies.

6.3.3 London Community Risk Register

Title: London Community Risk Register
Author(s): London Risk Advisory Group
Organization: London Risk Advisory Group
Publisher: Unavailable
Publishing Location: United Kingdom
Edition: N/A
Pages: 33
Retrieved from: London Fire Brigade website
Hyperlink: http://www.london-fire.gov.uk/Documents/LondonCommunityRiskRegister.pdf
Date of Publication: February 2010

Purpose:

- "The London Community Risk Register has been created to provide public information about hazards identified which could potentially have an impact upon London." [p.1]

Scope:

- This Risk Register only considers non-malicious events (hazards), and not threats. These hazards are rated for a worst case scenario in order to aid emergency services in preparing for events of similar or smaller scale.

Description:

- This document provides an overview of London's top three risks: severe weather, human health, and energy supply disruption.
- For each of the scenarios, the risk register provides an overview of the hazard, as well as advice on actions to take before, during, and after the incident.
- In addition, the document provides families and businesses with general guidance to prepare for emergencies. Lastly, there is a brief explanation on the purpose of risk assessments.

6.3.4 Assessing the Risk of Terrorist Attacks on Nuclear Facilities

Title: Assessing the Risk of Terrorist Attacks on Nuclear Facilities
Author(s): Parliamentary Office of Science and Technology (POST)
Organization: Parliamentary Office of Science and Technology (POST)
Publisher: Parliamentary Office of Science and Technology (POST)
Publishing Location: United Kingdom
Edition: N/A
Pages: 148
Retrieved from: Parliamentary Office of Science and Technology Report 222
Hyperlink: http://www.parliament.uk/briefing-papers/POST-Report-8
Date of Publication: July 2004

Objective:

- "The events of September 11th 2001 heightened concerns over the potential for terrorist attacks on nuclear facilities. The purpose of this report is to provide Parliamentarians with an overview of what is publicly known about the risks and the consequences of such an attack, either at a facility in the UK, or overseas, with very direct impacts in the UK.
- This report identifies the main issues of concern according to reports in the public domain, and highlights areas where understanding is limited due to lack of publicly available information." [Summary]

Scope:

- "The report focuses on the risk of sabotage of nuclear installations and shipments of radioactive material, both in the UK and overseas, with impacts on the UK. It does not provide a detailed discussion of the risk of theft of radioactive material." [p. 1-2]

Additional Information:
This report is structured as follows:

- Chapter 2: Describes the activities and facilities involving radioactive material
- Chapter 3: Discusses the regulations which seek to minimise risks of activities involving radioactive material
- Chapter 4-7: Presents the components that must be considered for assessing threat:
    - Intelligence
    - Vulnerability
    - Security
    - Consequences
- Chapters 8-10: Reviews three types of nuclear facilities:
    - Nuclear reactors
    - Reprocessing plants
    - Transporting of radioactive material
- Chapter 11: Describes existing knowledge on emergency arrangements in the UK, and provides a summary of international arrangements

6.4 Australia

6.4.1 State Summary: The Tasmanian Emergency Risk Management Project

Title: State Summary: The Tasmanian Emergency Risk Management Project
Author(s): State Emergency Service, Gilmour, R. (Ed)
Organization: State Emergency Service
Publisher: State Emergency Service
Publishing Location: Hobart, Tasmania, AU
Edition: Unavailable
Pages: 24
Retrieved from: State Emergency Service - Tasmania website
Hyperlink: http://www.ses.tas.gov.au/Library/StateSummaryFinal.pdf
Date of Publication: 2003

Purpose:
The aim of the Tasmanian Emergency Risk Management Project was to "utilise the Emergency Risk Management Guidelines to produce a risk assessment and risk treatment/mitigation study for the three regions of Tasmania based on community input." [p. 4]

Description:
- This document provides a summary of the Tasmanian Emergency Risk Management Project.

Additional Information:
This summary report provides:
- Overview of the Tasmanian Emergency Risk management Project
- Description of the steps of the Emergency Risk Management Process:
  - Establish the context
  - Identify risks
  - Analyze risks
  - Evaluate risks
  - Treat risks
- Main Natural Disaster Risk Findings:
  - Flood
  - Wildfire
  - Storm
  - Severe Weather
  - Earthquake/landslip
- Next steps

6.4.2 Natural Hazard Risk in Perth, Western Australia

Title: Natural Hazard Risk in Perth, Western Australia
Author(s): Senior Author: Trevor Jones
Compiled by Trevor Jones, Miriam Middelmann and Neil Corby
Organization: Geoscience Australia, Western Australia Fire and Emergency Services Authority (FESA), the Western Australia Department for Planning and Infrastructure (DPI), and the Bureau of Meteorology (BOM) through its Western Australia Regional Office
Publisher: Australian Government
Publishing Location: Australia
Edition: Unavailable
Pages: 352
Retrieved from: Australian Government website, Free Data Downloads (Geoscience Australia Publication - Report)
Hyperlink:
https://www.ga.gov.au/products/servlet/controller?event=GEOCAT_DETAILS&catno=63527
Date of Publication: 28 October 2009

Abstract:
"This report is a major risk assessment project based on metropolitan Perth, the capital city of Western Australia. Completed in June 2005, the report is the final publication in Geoscience Australia's Cities Project. Approximately 72% of Western Australia's population of around 1.3 million live in the Perth metropolitan area. Significant areas of Perth are situated along the banks of the flood prone Swan River and close to Australia's most active earthquake zone. There are several limestone belts to the north and south of Perth where karst systems have been discovered and the city's coastline suffers from coastal erosion as a result of high winds and fierce storms.
The study aimed at estimating the impact on the Perth community of several sudden-onset natural hazards. The natural hazards considered are both meteorological and terrestrial in origin. The hazards investigated most comprehensively are riverine floods in the Swan and Canning Rivers, severe winds in metropolitan Perth, and earthquakes in the Perth region. Some socioeconomic factors affecting the capacity of the citizens of Perth to recover from natural disaster events have been analysed and the WA data compared with data from other Australian states. Additionally, new estimates of earthquake hazard have been made in a zone of radius around 200km from Perth, extending east into the central Wheatbelt. The susceptibility of the southwest WA coastline to sea level rise from climate change has also been investigated. A commentary on the tsunami risk to WA coastline communities is also included.[28]"

Description:
- This report provides a description of risk assessment methods and their results for the following hazards: meteorological hazards, wind hazard, riverine flood hazard, earthquake risk, community recovery, and potential coastal erosion of the Swan coastal plain due to long-term sea level rise. For each of these risks, the report also provides risk management recommendations directed towards state and local governments.

Additional Information:
- The study developed more than a dozen major spatial databases and risk assessment models. Descriptions of several of these models can be found in the annexes.

[28] From https://www.ga.gov.au/products/servlet/controller?event=GEOCAT_DETAILS&catno=63527

6.4.3 Bayside City Council, Community Emergency Risk Management Plan

Title: Bayside City Council, Community Emergency Risk Management Plan
Author(s): Emergency Management Consultancy Services Pty Ltd.
Organization: Bayside City Council
Publisher: Unavailable
Publishing Location: Unavailable
Edition: Unavailable
Pages: 52
Retrieved from: Bayside city council website
Hyperlink:http://www.bayside.vic.gov.au/(9)_Part_C1_-_CERM_Jul_2011.pdf
Date of Publication: Unavailable, but last amended May 2011

Purpose:

- "This workbook has been developed to record the decisions of the Municipal Emergency Management Planning Committee (MEMPC) Risk Assessment Sub Group. This group included input from representatives of external organisations that do not sit on the MEMPC. The workbook details the process undertaken to identify, analyse, rate and treat each of the risks that may impact on the municipality." [p. 1]

Description:

- This report identifies 18 risks, for which the authors have assigned a risk rating.
- For each of these risks, the workbook contains a risk register outlining the consequence and likelihood rating, a risk statement, controls and responsible organisations, and treatment strategies.

6.4.4 City of Mitcham, Community Emergency Risk Management (CERM) Action Plan

Title: City of Mitcham, Community Emergency Risk Management (CERM) Action Plan
Author(s): City of Mitcham
Organization: City of Mitcham
Publisher: City of Mitcham
Publishing Location: Mitcham, Australia
Edition: Unavailable
Pages: 68
Retrieved from: City of Mitcham website
Hyperlink: http://www.mitchamcouncil.sa.gov.au/webdata/resources/files/Action_plan__final.pdf
Date of Publication: December 2004

Purpose:

- This Action Plan is the result of the City of Mitcham's Community Emergency Risk Management pilot project. The aim of the project is: "With direct community input, develop an action plan which identifies strategies to reduce the risk of hazards that have potential to impact on the Mitcham community." [p.7]

Description:

- This document provides background information on risk management as well as a community profile for the City of Mitcham.
- It describes the principal consultation strategies, in which the role of the community is emphasized.
- Next, it provides a brief overview of the top 20 priority risks for households and businesses.
- The report then provides tables which summarize the results of risk analysis, evaluation and treatment for a list of risk statements.
- These risk statements are divided into the following categories: infrastructure, workplace, environment, crime and safety and emergency events.

6.4.5 Community Risk in Mackay: A Multi-Hazard Risk Assessment

Title: Community Risk in Mackay: A Multi-Hazard Risk Assessment
Author(s): Miriam Middelmann and Ken Granger (editors)
Organization: Australian Geological Survey Organisation
Publisher: Australian Geological Survey Organisation
Publishing Location: Australia
Edition: Unavailable
Pages: 16
Retrieved from: Geoscience Australia website
Hyperlink: http://www.ga.gov.au/image_cache/GA4186.pdf
Date of Publication: 2000

Audience:

- "The report will be a valuable resource to those responsible for, or interested in, the management of these risks." [p. 1]

Scope:

- "Increased community safety, and consequently more sustainable and prosperous communities is the primary focus of this research." [p. 1]

Description:

- This report presents the results of a risk assessment study conducted in the community of Mackay.
- The full report is available on Compact Disk.

Additional Information:
This document contains the following sections:

- Background
- Community vulnerability (5 elements at risk in the community)
- Earthquake risk
- Flood risk
- Cyclone risk
- Risk evaluation
- Is Mackay a risky place?
- Strategies

6.5 Netherlands

6.5.1 Flood Risk Assessment in the Netherlands: A Case Study for Dike Ring South Holland

Title: Flood Risk Assessment in the Netherlands: A Case Study for Dike Ring South Holland
Author(s): Sebastiaan N. Jonkman, Matthijs Kok, and Johannes K. Vrijling
Organization: N/A
Publisher: Wiley-Blackwell
Publishing Location: Unavailable
Edition: N/A
Pages: 1357-1374
Retrieved from: Risk Analysis, Vol. 28, No. 5
Hyperlink: N/A
Date of Publication: October 2008

Abstract:
"Large parts of the Netherlands are below sea level. Therefore, it is important to have insight into the possible consequences and risks of flooding. In this article, an analysis of the risks due to flooding of the dike ring area South Holland in the Netherlands is presented. For different flood scenarios the potential number of fatalities is estimated. Results indicate that a flood event in this area can expose large and densely populated areas and result in hundreds to thousands of fatalities. Evacuation of South Holland before a coastal flood will be difficult due to the large amount of time required for evacuation and the limited time available. By combination with available information regarding the probability of occurrence of different flood scenarios, the flood risks have been quantified. The probability of death for a person in South Holland due to flooding, the so-called individual risk, is small. The probability of a flood disaster with many fatalities, the so-called societal risk, is relatively large in comparison with the societal risks in other sectors in the Netherlands, such as the chemical sector and aviation. The societal risk of flooding appears to be unacceptable according to some of the existing risk limits that have been proposed in literature. These results indicate the necessity of a further societal discussion on the acceptable level of flood risk in the Netherlands and the need for additional risk reducing measures." [p. 1357]

Key words: Flood defense; flood risk; loss of life; quantitative risk analysis; risk evaluation

6.5.2 Flood Risk Calculated with Different Risk Measures

Title: Flood Risk Calculated with Different Risk Measures
Author(s): S.N. Jonkman, P.H.A.J.M. van Gelder, J.K. Vrijling
Organization: N/A
Publisher: Unavailable
Publishing Location: Unavailable
Edition: N/A
Pages: 2360-2372
Retrieved from: Coastal Engineering 2002: Solving Coastal Conundrums - Proceedings of the 28th International Conference, Vol. 2
Hyperlink: N/A
Date of Publication: 2002

Abstract:
"In this paper it is investigated whether flood risks of an existing area in the Netherlands can be determined with different risk measures. An overview is given of risk measures used in the field of quantitative risk analysis. Furthermore, a case study is described, in which a flood risk analysis is performed. The results of these risk calculations are compared to existing standards and the risks of other activities in the Netherlands." [p. 2360]

Additional Information:
This paper offers:

- Summary of quantitative risk measures: individual risk measures, societal risk measures, economic risk measures (Includes a summary chart of these measures)
- Overview and description of the Pilot Case Flood Risk (PICASO)
- Calculation of flood risk for an existing polder in the Netherlands.
- Discussion on the possibility for applying risk measures in decision-making

6.6 Miscellaneous

6.6.1 ECDC Risk Assessment - 2009 Influenza A (H1N1) Pandemic

Title: ECDC Risk Assessment - 2009 Influenza A (H1N1) Pandemic
Author(s): European Centre for Disease Prevention and Control (ECDC)
Organization: European Centre for Disease Prevention and Control (ECDC)
Publisher: European Centre for Disease Prevention and Control (ECDC)
Publishing Location: Stockholm, Sweden
Edition: Version 7
Pages: 27
Retrieved from: European Centre for Disease Prevention and Control website
Hyperlink:
http://ecdc.europa.eu/en/healthtopics/Documents/0908_Influenza_AH1N1_Risk_Assessment.pdf
Date of Publication: December 17, 2009

Description:

- This document presents an update of the ECDC pandemic risk assessment for Europe, more specifically, for the 2009 Influenza A (H1N1) Pandemic.

Additional Information:
This document covers the following topics:

- Background
- Important features
  - Basic epidemiology and basic parameters
  - Disease characteristics
  - Features of the Virus
- Areas of particular uncertainty
- Next steps for ECDC

7 Summary

As a part of the collaborative project between Emergency Management British Columbia (EMBC) and Defence Research and Development Canada (DRDC), extensive literature searches in risk assessment (RA) and critical infrastructure (CI) were performed. This document presents the results of a literature search for RA. The literature search comprises a collection of almost 200 references on RA that are relevant to public safety and security. These references include standards, government publications, academic papers, and reports produced by practitioners and non-governmental or private sector organizations. The document is intended to be a reference for DRDC, EMBC and external partners. The organization and description of the literature should allow users to identify and retrieve those references which are most relevant to their work and interests.

References

[1] International Organization for Standardization (ISO). (n.d.). *Standards*. Retrieved from http://www.iso.org/iso/home/standards.htm

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, for example Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)
Centre for Security Science Defence R&D Canada 222 Nepean St. 11th Floor Ottawa, ON Canada K1A 0K2	UNCLASSIFIED NON-CONTROLLED GOODS DMC A Review: ECL June 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Risk Assessment References: Documented Literature Search

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Pak, K., Genik, L.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2012	202	20

7. DESCRIPTIVE NOTES (The category of the document, for example technical report, technical note or memorandum. If appropriate, enter the type of report, for example interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Note

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science

Defence R&D Canada

222 Nepean St. 11th Floor

Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
File 3700-1	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TN 2012-014	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement

audience may be selected.))

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This document presents the results of a literature search for risk assessment (RA) as it pertains to public safety and security, and was undertaken as part of a collaborative project between Defence Research & Development Canada (DRDC) and Emergency Management British Columbia (EMBC). It consists of bibliographic information, abstracts, and key points for almost 200 references, organized into the following categories: standards; frameworks and guidelines; methodologies, tools, and models; academic discussions; and case studies. The references include standards, government publications, academic papers, and reports produced by practitioners and non-governmental or private sector organizations, and were categorized, ordered and described to assist readers in selecting and retrieving references that may be of value to their work. This document is intended to be a resource for DRDC, EMBC and other external partners.

Ce document présente les résultats d'une recherche documentaire sur l'évaluation des risques associés à la sécurité publique. Cette recherche a été menée dans le cadre d'un projet de collaboration entre Recherche et développement pour la défense Canada (RDDC) et Emergency Management British Columbia (EMBC). Des renseignements bibliographiques, des extraits et des faits saillants de près de 200 documents de références sont classés par catégorie : normes; cadre et lignes directrices; méthodologies, outils et modèles; discussions universitaires; études de cas. Les documents de références incluent des normes, des publications gouvernementales, des recherches universitaires et des rapports rédigés par des organisations professionnelles, non gouvernementales et du secteur privé. Ils ont été classés, organisés et décrits dans le but d'aider le lecteur à sélectionner et à trouver des documents de référence pouvant lui être utile. Il s'agit d'un outil que RDDC, EMBC et d'autres partenaires externes peuvent utiliser comme ressource.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, for example Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Risk Assessment; Literature Search